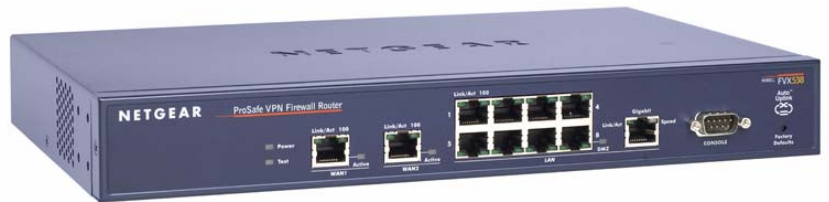


ProSafe VPN Firewall 200 FVX538 Reference Manual



NETGEAR®

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

August 2006
202-10062-04
v1.0

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks and ProSafe is a trademark of NETGEAR, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

EU Regulatory Compliance Statement

ProSafe VPN Firewall 200 is compliant with the following EU Council Directives: 89/336/EEC and LVD 73/23/EEC. Compliance is verified by testing to the following standards: EN55022 Class B, EN55024 and EN60950-1.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das ProSafe VPN Firewall 200 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the ProSafe VPN Firewall 200 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

Additional Copyrights

AES	<p>Copyright (c) 2001, Dr Brian Gladman <brg@gladman.uk.net>, Worcester, UK. All rights reserved.</p> <p>TERMS</p> <p>Redistribution and use in source and binary forms, with or without modification, are permitted subject to the following conditions:</p> <ol style="list-style-type: none">1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.3. The copyright holder's name must not be used to endorse or promote any products derived from this software without his specific prior written permission. <p>This software is provided 'as is' with no express or implied warranties of correctness or fitness for purpose.</p>
-----	--

Open SSL	<p>Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved.</p> <p>Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions * are met:</p> <ol style="list-style-type: none"> 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)" 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org. 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project. 6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)" <p>THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.</p> <p>This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).</p>
----------	--

MD5	<p>Copyright (C) 1990, RSA Data Security, Inc. All rights reserved.</p> <p>License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.</p> <p>RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.</p> <p>These notices must be retained in any copies of any part of this documentation and/or software.</p>
PPP	<p>Copyright (c) 1989 Carnegie Mellon University. All rights reserved.</p> <p>Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Carnegie Mellon University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.</p> <p>THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.</p>
Zlib	<p>zlib.h -- interface of the 'zlib' general purpose compression library version 1.1.4, March 11th, 2002. Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler.</p> <p>This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:</p> <ol style="list-style-type: none"> 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution. <p>Jean-loup Gailly: jloup@gzip.org; Mark Adler: madler@alumni.caltech.edu</p> <p>The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files ftp://ds.internic.net/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format)</p>

Product and Publication Details

Model Number:	FVX538
Publication Date:	August 2006
Product Family:	VPN Firewall
Product Name:	ProSafe VPN Firewall 200
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10062-04
Publication Version Number	1.0

Contents

About This Manual

Conventions, Formats and Scope	xiii
How to Use This Manual	xiv
How to Print this Manual	xiv
Revision History	xv

Chapter 1

Introduction

Key Features	1-1
Dual WAN Ports for Increased Reliability or Outbound Load Balancing	1-2
A Powerful, True Firewall with Content Filtering	1-2
Security Features	1-3
Autosensing Ethernet Connections with Auto Uplink	1-3
Extensive Protocol Support	1-3
Trend Micro Integration	1-4
Easy Installation and Management	1-4
Maintenance and Support	1-5
Package Contents	1-5
Router Front Panel	1-6
Router Rear Panel	1-8
Rack Mounting Hardware	1-9
The Router's IP Address, Login Name, and Password	1-9
Default Log In Settings	1-10

Chapter 2

Connecting the FVX538 to the Internet

Logging into the VPN Firewall	2-1
Configuring the Internet Connections to Your ISPs	2-2
Setting the Router's MAC Address	2-5
Manually Configuring Your Internet Connection	2-5

Programming the Traffic Meter (if Desired)	2-7
Configuring the WAN Mode (Required for Dual WAN)	2-10
Setting Up Auto-Rollover Mode	2-11
Setting Up Load Balancing	2-13
Configuring Dynamic DNS (If Needed)	2-15
Configuring the Advanced WAN Options (If Needed)	2-18

Chapter 3

LAN Configuration

Using the Firewall as a DHCP server	3-1
Configuring the LAN Setup Options	3-2
Configuring Multi Home LAN IPs	3-4
Managing Groups and Hosts (LAN Groups)	3-6
Creating the Network Database	3-6
Setting Up Address Reservation	3-9
Configuring and Enabling the DMZ Port	3-10
Static Routes	3-12
Configuring Static Routes	3-12
Routing Information Protocol (RIP)	3-13
Static Route Example	3-15
Enabling Trend Micro Antivirus Enforcement	3-15

Chapter 4

Firewall Protection and Content Filtering

Using Rules to Block or Allow Specific Kinds of Traffic	4-1
Services-Based Rules	4-2
Outbound Rules (Service Blocking)	4-2
Inbound Rules (Port Forwarding)	4-4
Order of Precedence for Rules	4-7
Setting LAN WAN Rules	4-7
LAN WAN Outbound Services Rules	4-9
LAN WAN Inbound Services Rules	4-10
Setting DMZ WAN Rules	4-10
Setting LAN DMZ Rules	4-12
LAN DMZ Outbound Services Rules	4-13
LAN DMZ Inbound Services Rules	4-14
Attack Checks	4-14

Inbound Rules Examples	4-16
LAN WAN Inbound Rule: Hosting A Local Public Web Server	4-16
LAN WAN Inbound Rule: Allowing Videoconference from Restricted Addresses	4-17
LAN WAN or DMZ WAN Inbound Rule: Setting Up One-to-One NAT Mapping	4-17
LAN WAN or DMZ WAN Inbound Rule: Specifying an Exposed Host	4-19
Outbound Rules Example	4-20
LAN WAN Outbound Rule: Blocking Instant Messenger	4-20
Adding Customized Services	4-21
Setting Quality of Service (QoS) Priorities	4-23
Setting a Schedule to Block or Allow Specific Traffic	4-24
Setting Block Sites (Content Filtering)	4-25
Enabling Source MAC Filtering	4-27
Port Triggering	4-28
E-Mail Notifications of Event Logs and Alerts	4-31
Administrator Tips	4-35

Chapter 5

Virtual Private Networking

Dual WAN Port Systems	5-1
Setting up a VPN Connection using the VPN Wizard	5-3
Creating a VPN Tunnel to a Gateway	5-4
Creating a VPN Tunnel Connection to a VPN Client	5-7
VPN Tunnel Policies	5-10
IKE Policy	5-10
Managing IKE Policies	5-11
IKE Policy Table	5-11
VPN Policy	5-12
Managing VPN Policies	5-12
VPN Policy Table	5-13
VPN Tunnel Connection Status	5-13
Creating a VPN Gateway Connection: Between FVX538 and FVS338	5-14
Configuring the FVX538	5-14
Configuring the FVS338	5-19
Testing the Connection	5-20
Creating a VPN Client Connection: VPN Client to FVX538	5-20
Configuring the FVX538	5-20

Configuring the VPN Client	5-22
Testing the Connection	5-26
Certificate Authorities	5-27
Generating a Self Certificate Request	5-28
Uploading a Trusted Certificate	5-30
Managing your Certificate Revocation List (CRL)	5-30
Extended Authentication (XAUTH) Configuration	5-31
Configuring XAUTH for VPN Clients	5-32
User Database Configuration	5-34
RADIUS Client Configuration	5-35
Manually Assigning IP Addresses to Remote Users (ModeConfig)	5-37
Mode Config Operation	5-37
Configuring the VPN Firewall	5-38
Configuring the ProSafe VPN Client for ModeConfig	5-41

Chapter 6

Router and Network Management

Performance Management	6-1
Bandwidth Capacity	6-1
VPN Firewall Features That Reduce Traffic	6-2
Service Blocking	6-2
Block Sites	6-4
Source MAC Filtering	6-4
VPN Firewall Features That Increase Traffic	6-5
Port Forwarding	6-5
Port Triggering	6-6
DMZ Port	6-7
VPN Tunnels	6-7
Using QoS to Shift the Traffic Mix	6-7
Tools for Traffic Management	6-8
Administration	6-8
Changing Passwords and Settings	6-8
Enabling Remote Management Access	6-10
Using a SNMP Manager	6-11
Settings Backup and Firmware Upgrade	6-13
Backup and Restore Settings	6-14

Router Upgrade	6-15
Setting the Time Zone	6-16
Monitoring the Router	6-17
Enabling the Traffic Meter	6-17
Setting Login Failures and Attacks Notification	6-19
Monitoring Attached Devices	6-20
Viewing Port Triggering Status	6-22
Viewing Router Configuration and System Status	6-23
Monitoring WAN Ports Status	6-24
Monitoring VPN Tunnel Connection Status	6-25
VPN Logs	6-26
DHCP Log	6-27
Performing Diagnostics	6-27

Chapter 7

Troubleshooting

Basic Functions	7-1
Power LED Not On	7-1
LEDs Never Turn Off	7-2
LAN or Internet Port LEDs Not On	7-2
Troubleshooting the Web Configuration Interface	7-2
Troubleshooting the ISP Connection	7-4
Troubleshooting a TCP/IP Network Using a Ping Utility	7-5
Testing the LAN Path to Your Firewall	7-5
Testing the Path from Your PC to a Remote Device	7-6
Restoring the Default Configuration and Password	7-7
Problems with Date and Time	7-7

Appendix A

Default Settings and Technical Specifications

Appendix B

Related Documents

Appendix C

Network Planning for Dual WAN Ports

What You Will Need to Do Before You Begin	C-1
Cabling and Computer Hardware Requirements	C-3
Computer Network Configuration Requirements	C-3

Internet Configuration Requirements	C-3
Where Do I Get the Internet Configuration Parameters?	C-4
Internet Connection Information Form	C-5
Overview of the Planning Process	C-6
Inbound Traffic	C-6
Virtual Private Networks (VPNs)	C-6
The Roll-over Case for Firewalls With Dual WAN Ports	C-7
The Load Balancing Case for Firewalls With Dual WAN Ports	C-7
Inbound Traffic	C-8
Inbound Traffic to Single WAN Port (Reference Case)	C-8
Inbound Traffic to Dual WAN Port Systems	C-8
Inbound Traffic: Dual WAN Ports for Improved Reliability	C-9
Inbound Traffic: Dual WAN Ports for Load Balancing	C-9
Virtual Private Networks (VPNs)	C-10
VPN Road Warrior (Client-to-Gateway)	C-11
VPN Road Warrior: Single Gateway WAN Port (Reference Case)	C-12
VPN Road Warrior: Dual Gateway WAN Ports for Improved Reliability	C-12
VPN Road Warrior: Dual Gateway WAN Ports for Load Balancing	C-13
VPN Gateway-to-Gateway	C-14
VPN Gateway-to-Gateway: Single Gateway WAN Ports (Reference Case) ..	C-14
VPN Gateway-to-Gateway: Dual Gateway WAN Ports for Improved Reliability	C-15
VPN Gateway-to-Gateway: Dual Gateway WAN Ports for Load Balancing ...	C-17
VPN Telecommuter (Client-to-Gateway Through a NAT Router)	C-17
VPN Telecommuter: Single Gateway WAN Port (Reference Case)	C-18
VPN Telecommuter: Dual Gateway WAN Ports for Improved Reliability	C-18
VPN Telecommuter: Dual Gateway WAN Ports for Load Balancing	C-20

Index

About This Manual

The *NETGEAR® ProSafe™ VPN Firewall 200* describes how to install, configure and troubleshoot the ProSafe VPN Firewall 200. The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats and Scope


The conventions, formats, and scope of this manual are described in the following paragraphs.


- **Typographical Conventions.** This manual uses the following typographical conventions:


<i>Italics</i>	Emphasis, books, CDs, URL names
Bold	User input
Fixed	Screen text, file and server names, extensions, commands, IP addresses

- **Formats.** This manual uses the following formats to highlight special messages:

	Note: This format is used to highlight information of importance or special interest.
---	--

	Tip: This format is used to highlight a procedure that will save time or resources.
---	--

	Warning: Ignoring this type of note may result in a malfunction or damage to the equipment.
---	--

	Danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.
---	--

- **Scope.** This manual is written for the VPN firewall according to the following specifications:

Product Version	ProSafe VPN Firewall 200
Manual Publication Date	August 2006





For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in [Appendix B, “Related Documents.”](#)



Note: Updates to this product are available on the NETGEAR, Inc. website at <http://kbserver.netgear.com/products/FVX538.asp>.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons,  and , for browsing forward or backward through the manual one page at a time.
- A  button that displays the table of contents and a  button that displays the Index. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A  button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual you can choose one of the following options, according to your needs.

- **Printing a Page from HTML.** Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.
- **Printing from PDF.** Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at <http://www.adobe.com>.
 - **Printing a PDF Chapter.** Use the *PDF of This Chapter* link at the top left of any page.

- Click the *PDF of This Chapter* link at the top left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
 - Click the print icon in the upper left of your browser window.
- **Printing a PDF version of the Complete Manual.** Use the *Complete PDF Manual* link at the top left of any page.
- Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
 - Click the print icon in the upper left of your browser window.



Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Revision History

Part Number	Version Number	Description
202-10062-04	1.0	Product update: New firmware and a new user interface.

Chapter 1

Introduction

The ProSafe VPN Firewall 200 with eight 10/100 ports and one 1/100/1000 port connects your local area network (LAN) to the Internet through an external access device such as a cable modem or DSL modem.

The FVX538 is a complete security solution that protects your network from attacks and intrusions. For example, the FVX538 provides support for Stateful Packet Inspection, Denial of Service (DoS) attack protection and multi-NAT support. The VPN firewall supports multiple Web content filtering options, plus browsing activity reporting and instant alerts—both via e-mail. Network administrators can establish restricted access policies based on time-of-day, Website addresses and address keywords.

The FVX538 is a plug-and-play device that can be installed and configured within minutes.

Key Features

The VPN firewall provides the following features:

- Dual 10/100 Mbps Ethernet WAN ports for load balancing or failover protection, providing increased system reliability, load balancing, or link aggregation. The WAN ports do not respond at all to unsolicited traffic (stealth mode).
- Support for up to 200 simultaneous IPSec VPN tunnels.
- Bundled with the 5-user license of the NETGEAR ProSafe VPN Client software (VPN05L)
- Proactive policy enforcement for anti-virus and anti-spam security with integrated Trend Micro support.
- Quality of Service (QoS) and SIP 2.0 support for traffic prioritization, voice, and multimedia.
- Built-in 10/100 Mbps ports plus 1 Gigabit Switch port.
- One console port for local management.
- SNMP Manageable, optimized for the NETGEAR ProSafe Network Management Software (NMS100).
- Easy, web-based setup for installation and management.
- Advanced SPI Firewall and Multi-NAT support.
- Extensive Protocol Support.

- Login capability.
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrade.
- One U Rack mountable.

Dual WAN Ports for Increased Reliability or Outbound Load Balancing

The FVX538 has two broadband WAN ports, WAN1 and WAN2, each capable of operating independently at speeds of either 10 Mbps or 100 Mbps. The two WAN ports let you connect a second broadband Internet line that can be configured on a mutually-exclusive basis to:

- Provide backup and rollover if one line is inoperable, ensuring you are never disconnected.
- Load balance, or use both Internet lines simultaneously for the outgoing traffic. The firewall balances users between the two lines for maximum bandwidth efficiency.

See [“Network Planning for Dual WAN Ports” on page C-1](#) for the planning factors to consider when implementing the following capabilities with dual WAN port gateways:

- Single or multiple exposed hosts
- Virtual private networks

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the FVX538 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- **DoS protection.** Automatically detects and thwarts DoS attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.
- **Secure Firewall.** Blocks unwanted traffic from the Internet to your LAN.
- **Block Sites.** Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- **Logs security incidents.** The FVX538 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your email address or email pager whenever a significant event occurs.

- **Keyword Filtering.** With its URL keyword filtering feature, the FVX538 prevents objectionable content from reaching your PCs. The firewall allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the firewall to log and report attempts to access objectionable Internet sites.

Security Features

The VPN firewall is equipped with several features designed to maintain security, as described in this section.

- **PCs Hidden by NAT.** NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the PCs on the LAN.
- **Port Forwarding with NAT.** Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the firewall allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request. You can specify forwarding of single ports or ranges of ports.
- **DMZ port.** Incoming traffic from the Internet is normally discarded by the firewall unless the traffic is a response to one of your local computers or a service for which you have configured an inbound rule. Instead of discarding this traffic, you can have it forwarded to one computer on your network.

Autosensing Ethernet Connections with Auto Uplink

With its internal 8-port 10/100 switch, the FVX538 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The firewall incorporates Auto Uplink™ technology. Each Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a ‘normal’ connection such as to a PC or an ‘uplink’ connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Extensive Protocol Support

The VPN firewall supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, refer to *“Internet Configuration Requirements” in Appendix C.*

- **IP Address Sharing by NAT.** The VPN firewall allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as NAT, allows the use of an inexpensive single-user ISP account.
- **Automatic Configuration of Attached PCs by DHCP.** The VPN firewall dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.
- **DNS Proxy.** When DHCP is enabled and no DNS addresses are specified, the firewall provides its own address as a DNS server to the attached PCs. The firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- **PPP over Ethernet (PPPoE).** PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as EnterNet or WinPOET on your PC.

Trend Micro Integration

If you have installed the Trend Micro Client/Server/Messaging Suite for SMB on your local network, you can have the firewall enforce its use. When Antivirus Enforcement is selected, local PCs will not be allowed Web access unless they have the Trend Micro OfficeScan client installed and updated with the latest virus definitions.

The Client/Server/Messaging Suite for Small and Medium Business protects file servers, mail servers, and PCs on your network—including antispam capability. The Client/Server Suite for Small and Medium Business protects files servers and PCs.

- Both products deliver a layered defense against viruses and other malicious code.
- Unlike competing antivirus products, both products work your NETGEAR VPN Firewall to enforce antivirus policies - end users cannot access the Internet unless they have antivirus protection with current pattern files installed.
- Both products are specifically built to meet the needs of growing businesses and feature easy installation, automatic transparent updates, and damage cleanup capability.
- Activate either product for a free trial.

Easy Installation and Management

You can install, configure, and operate the ProSafe VPN Firewall 200 within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-Based Management.** Browser-based configuration allows you to easily configure your firewall from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- **Auto Detect.** The VPN firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **VPN Wizard.** The VPN firewall includes the NETGEAR VPN Wizard to easily configure VPN tunnels according to the recommendations of the Virtual Private Network Consortium (VPNC) to ensure the VPN tunnels are interoperable with other VPNC-compliant VPN routers and clients.
- **SNMP.** The VPN firewall supports the Simple Network Management Protocol (SNMP) to let you monitor and manage log resources from an SNMP-compliant system manager. The SNMP system configuration lets you change the system variables for MIB2.
- **Diagnostic Functions.** The firewall incorporates built-in diagnostic functions such as Ping, Trace Route, DNS lookup, and remote reboot.
- **Remote Management.** The firewall allows you to login to the Web Management Interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses, and you can choose a nonstandard port number.
- **Visual monitoring.** The VPN firewall's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the VPN firewall:

- Flash memory for firmware upgrade
- Free technical support seven days a week, 24 hours a day, according to the terms identified in the Warranty and Support information card provided with your product.

Package Contents

The product package should contain the following items:

- ProSafe VPN Firewall 200.
- AC power cable.

- 19-inch rack mounting hardware and rubber feet.
- Category 5 (Cat5) Ethernet cable.
- *Installation Guide, FVX538 ProSafe VPN Firewall 200*
- *Resource CD*, including:
 - Application Notes and other helpful information.
 - ProSafe VPN Client Software – five user licenses.
 - Trend Micro software evaluation.
- Warranty and Support Information Card.

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the firewall for repair.

Router Front Panel

The ProSafe VPN Firewall 200 front panel shown below contains the port connections, status LEDs, and the factory defaults reset button.

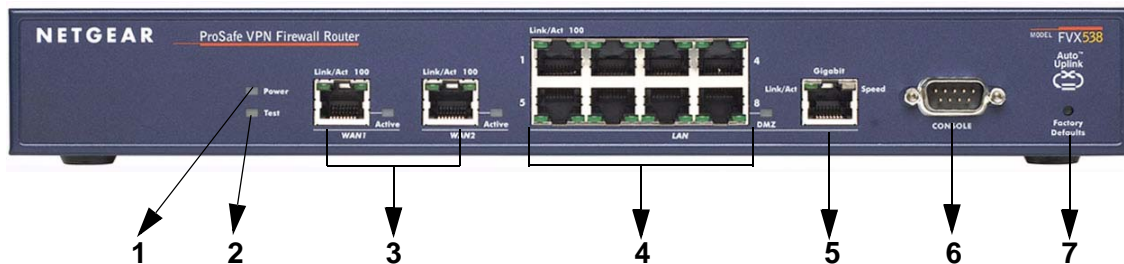


Figure 1-1

Table 1-1 describes each item on the front panel and its operation.

Table 1-1. Object Descriptions

Object	Activity	Description
1. Power LED	On (Green) Off	Power is supplied to the firewall. Power is not supplied to the firewall.
2. Test LED	On (Amber) Blinking (Amber) Off	Test mode: The system is initializing or the initialization has failed. Writing to Flash memory (during upgrading or resetting to defaults). The system has booted successfully.

Table 1-1. Object Descriptions (continued)

Object	Activity	Description
3. WAN Ports and LEDs	Two RJ-45 WAN ports	N-way automatic speed negotiation, Auto MDI/MDIX.
	Link/Act LED On (Green) Blinking (Green) Off	The WAN port has detected a link with a connected Ethernet device. Data is being transmitted or received by the WAN port. The WAN port has no link.
	100 LED On (Green) Off	The WAN port is operating at 100 Mbps. The WAN port is operating at 10 Mbps.
	Active LED On (Green) On (Amber) Off	The WAN port has a valid Internet connection. The Internet connection is down or not being used because the port is available for failover in case the connection on other WAN port fails. The WAN port is either not enabled or has no link.
4. LAN Ports and LEDs	8-port RJ-45 10/100 Mbps Fast Ethernet Switch	N-way automatic speed negotiation, auto MDI/MDIX.
	Link/Act LED On (Green) Blinking (Green) Off	The LAN port has detected a link with a connected Ethernet device. Data is being transmitted or received by the LAN port. The LAN port has no link.
	100 LED On (Green) Off	The LAN port is operating at 100 Mbps. The LAN port is operating at 10 Mbps.
	DMZ (port 8) On (Green) Off	Port 8 is operating as a dedicated hardware DMZ port. Port 8 is operating as a normal LAN port.
5. Gigabit Port and LEDs	Gbit RJ-45 connector	Port for connecting to a gigabit Ethernet device.
	Link/Act LED On (Green) Blinking (Green) Off	The LAN port has detected a link with a connected Ethernet device. Data is being transmitted or received by the LAN port. The LAN port has no link.
	Speed LED On (Green) On (Amber) Off	The LAN port is operating at 1,000 Mbps. The LAN port is operating at 100 Mbps. The LAN port is operating at 10 Mbps.

Table 1-1. Object Descriptions (continued)

Object	Activity	Description
6. Console Port	DB9 male connector	Port for connecting to an optional console terminal. Default baud rate is 115.2K; pinouts: (2) Tx, (3) Rx, (5) and (7) Gnd.
7. Factory Defaults	—> push in with a sharp object	Factory Defaults reset push button (see Appendix A, “Default Settings and Technical Specifications” for the factory defaults).

Router Rear Panel

The rear panel of the ProSafe VPN Firewall 200 ([Figure 1-2](#)) contains the On/Off switch and AC power connection.

**Figure 1-2**

Viewed from left to right, the rear panel contains the following elements:

1. AC power in
2. On/Off switch

Rack Mounting Hardware

The FVX538 can be mounted either on a desktop (using included rubber feet) or in a 19-inch rack (using the included rack mounting hardware illustrated in [Figure 1-3](#)).

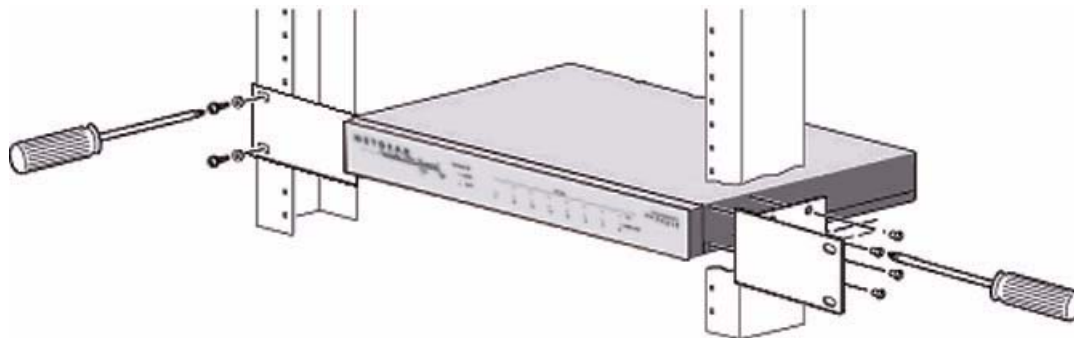


Figure 1-3

The Router's IP Address, Login Name, and Password

Check the label on the bottom of the FVX538's enclosure if you forget the following factory default information:

- IP Address: **http://192.168.1.1** to reach the Web-based GUI from the LAN
- User name: **admin**
- Password: **password**

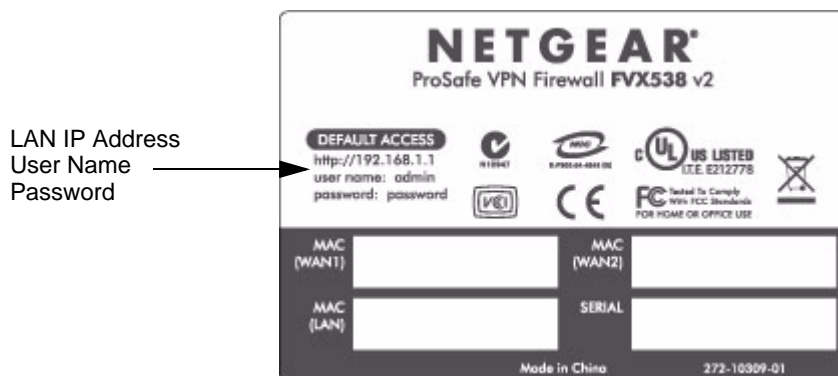


Figure 1-4

Default Log In Settings

To log in to the FVX538 once it is connected:

1. Open a Web browser.
2. Enter **http://192.168.1.1** as the URL.



Figure 1-5

3. Once the login screen displays ([Figure 1-5](#)), enter the following information:
 - **admin** for User Name
 - **password** for Password

Chapter 2

Connecting the FVX538 to the Internet

Typically, six steps are required to complete the basic connection of your firewall. Setting up VPN tunnels are covered in [Chapter 5, “Virtual Private Networking.”](#)

1. **Connect the firewall physically to your network.** Connect the cables, turn on your router and wait for the Test LED to go out. Make sure your Ethernet and LAN LEDs are lit. (See the *Installation Guide, FVX538 ProSafe VPN Firewall 200* for complete steps. A PDF of the *Installation Guide* is on the NETGEAR website at: <http://kbserver.netgear.com>.)
2. **Log in to the firewall.** After logging in, you are ready to set up and configure your firewall. You can also change your password and enable remote management at this time.
3. **Configure the Internet connections to your ISP(s).** During this phase, you will connect to your ISPs. You can also program the WAN traffic meters at this time if desired.
4. **Configure the WAN mode (required for dual WAN operation).** Select either auto-rollover mode or load balancing mode (on a mutually exclusive basis). For load balancing, you can also select the protocol bindings.
5. **Configure dynamic DNS on the WAN ports (if needed).** Configure your fully qualified domain names during this phase (if required).
6. **Configure the WAN options (if needed).** Optionally, you can enable each WAN port to respond to a ping. You can also change the factory default MTU size, port speed, and uplink bandwidth. However, these are advanced features and changing them is not usually required.

Logging into the VPN Firewall

To connect to the firewall, your computer needs to be configured to obtain an IP address automatically via DHCP. If you need instructions on how to configure your computer for DHCP, refer to the link in [Appendix B, “Related Documents.”](#)

To log in to the VPN firewall:

1. Connect to the firewall by typing **http://192.168.1.1** in the address field of Internet Explorer, Mozilla Firefox or Netscape® Navigator.

2. When prompted, enter **admin** for the firewall user name and **password** for the firewall password, both in lower case letters. (The firewall user name and password are not the same as any user name or password you may use to log in to your Internet connection.)
3. Click **Login**.



Note: You might want to enable remote management at this time so that you can log in remotely in the future to manage the firewall (see “[Enabling Remote Management Access](#)” on page 6-10). If you enable remote management, you are strongly advised to change your password (see “[Changing Passwords and Settings](#)” on page 6-8).

Configuring the Internet Connections to Your ISPs

You should first configure your Internet connections to your ISPs on WAN port 1, and then configure WAN port 2 second.

To automatically configure the WAN ports and connect to the Internet:

1. The **WAN1 ISP Settings** screen similar to the one shown in [Figure 2-1](#) should display when you log in. (If the screen does not display, select the primary menu option **Network Configuration** and the sub-menu option **WAN Settings**.)

The screenshot shows the 'WAN1 ISP Settings' configuration page. At the top, a navigation bar includes 'Network Configuration', 'Security', 'VPN', 'Administration', 'Monitoring', 'Web Support', and 'Logout'. Below this, a breadcrumb trail shows 'WAN Settings :: WAN Mode :: Protocol Binding :: Dynamic DNS :: LAN Setup :: LAN Groups :: DMZ Setup :: Routing'. The main content area is divided into several sections:

- ISP Login:** A section titled 'Does Your Internet Connection Require a Login?' with radio buttons for 'Yes' and 'No' (selected). It includes input fields for 'Login:' and 'Password:'.
- ISP Type:** A section titled 'Which type of ISP connection do you use?' with radio buttons for 'Austria (PPTP)', 'Other (PPPoE)' (selected), and 'BigPond Cable'. It includes input fields for 'Account Name:', 'Domain Name:', 'Login Server:', 'Idle Timeout:' (with 'Keep Connected' selected), 'Idle Time:' (set to 5 minutes), 'My IP Address:', and 'Server IP Address:'.
- Internet (IP) Address:** A section with radio buttons for 'Get Dynamically from ISP' (selected) and 'Use Static IP Address'. It includes input fields for 'IP Address:', 'IP Subnet Mask:', and 'Gateway IP Address:'.
- Domain Name Server (DNS) Servers:** A section with radio buttons for 'Get Automatically from ISP' (selected) and 'Use These DNS Servers'. It includes input fields for 'Primary DNS Server:' and 'Secondary DNS Server:'.

At the bottom of the page, there are four buttons: 'Apply', 'Reset', 'Test', and 'Auto Detect'. A dashed box highlights the 'Auto Detect' button, and an arrow points from it to the 'Operation succeeded.' message at the top of the page.

Figure 2-1

2. Click **Auto Detect** at the bottom of the screen to automatically detect the type of Internet connection provided by your ISP. Auto Detect will probe for different connection methods and suggest one that your ISP will most likely support.

When Auto Detect successfully detects an active Internet service, it reports which connection type it discovered. The options are described in the following table.

Table 2-1. Internet connection methods

Connection Method	Data Required
PPPoE	Login (Username, Password); Account Name, Domain Name
PPTP	Login (Username, Password), Account Name, Local IP address, and PPTP Server IP address;

Table 2-1. Internet connection methods (continued)


Connection Method	Data Required
BigPond Cable	Login Username, Password), Login Server.
DHCP (Dynamic IP)	No data is required.
Fixed (Static) IP	Static IP address, Subnet, and Gateway IP; and related data supplied by your ISP.

If Auto Detect does not find a connection, you will be prompted to check the physical connection between your firewall and the cable or DSL line or to check your Router's MAC address (see [“Setting the Router's MAC Address” on page 2-5](#)).

3. Click **WAN Status** at the top right of the screen to verify WAN Port 1 connection status. Click **Connect** if connection not already present.

**Figure 2-2**

4. Set up the traffic meter for WAN 1 ISP if desired. See [“Programming the Traffic Meter \(if Desired\)” on page 2-7](#).

	<p>Note: At this point of the configuration process, you are now connected to the Internet through WAN port 1. But you must continue with the configuration process to get the complete functionality of the dual WAN interface.</p>
---	---

The configure the **WAN2 ISP** settings:

1. Repeat the above steps to set up the parameters for WAN2 ISP. Start by selecting the WAN2 ISP Settings tab. Next click **Auto Detect** on the WAN2 ISP Settings screen and then confirm the connection by clicking the **WAN** Status link.
2. Set up the traffic meter for WAN2 ISP, if desired. See [“Programming the Traffic Meter \(if Desired\)” on page 2-7](#).

Setting the Router’s MAC Address

Each computer or router on your network has a unique 48-bit local Ethernet address. This is also referred to as the computer’s MAC (Media Access Control) address. The default is set to **Use Default Address**. If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, then you must enter that address. Setting the router’s MAC address is controlled through the **Advanced** options on the **WAN1 ISP Settings** and **WAN2 ISP Settings** screen (see [“Configuring the Advanced WAN Options \(If Needed\)” on page 2-18](#)).

Manually Configuring Your Internet Connection

If you know your ISP connection type, you can bypass the Auto Detect feature and connect your router manually. Ensure that you have all of the relevant connection information such as IP Addresses, account information, type of ISP connection, etc., before you begin. Unless your ISP automatically assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP (see [Figure 2-1](#)).



Note: To enable a WAN port to respond to a Ping from the Internet, use the Rules menu ([Figure 4-2 on page 4-8](#)).

To manually configure your **WAN1 ISP Settings**:

1. **Does your Internet connection require a login?** If you need to enter login information every time you connect to the Internet through your ISP, select Yes. Otherwise, select No.
2. **What type of IPS connection do you use?** If your connection is PPPoE, PPTP or BigPond Cable, then you must login. Check the Yes radio box. The text box fields that require data entry will be highlighted, based on the connection that you selected. If your ISP has not assigned any login information, then choose the No radio box and skip this section. For example:
 - **Austria (PPTP):** If your ISP is Austria Telecom or any other ISP that uses PPTP for login, select this. Then, fill in the following highlighted fields:

- **Account Name** (also known as Host Name or System Name): Enter the valid account name for the PPTP connection (usually your email “ID” assigned by your ISP). Some ISPs require entering your full email address here.
 - **Domain Name:** Your domain name or workgroup name assigned by your ISP, or your ISP’s domain name. You may leave this field blank.
 - **Idle Timeout:** Check the Keep Connected radio box to keep the connection always on. To logout after the connection is idle for a period of time, select Idle Time and enter the number of minutes to wait before disconnecting in the timeout field. This is useful if your ISP charges you based on the amount of time you have logged in.
 - **My IP Address:** IP address assigned by the ISP to make the connection with the ISP server.
 - **Server IP Address:** IP address of the PPTP server.
 - **Other (PPPoE):** If you have installed login software such as WinPoET or Enternet, then your connection type is PPPoE. Select this connection and configure the following fields:
 - **Account Name:** Valid account name for the PPPoE connection
 - **Domain Name:** Name of your ISP’s domain or your domain name if your ISP has assigned one. You may leave this field blank.
 - **Idle Timeout:** Select Keep Connected, to keep the connection always on. To logout after the connection is idle for a period of time, select Idle Time and enter the number of minutes to wait before disconnecting, in the timeout field.
 - **BigPond Cable:** If your ISP is Telstra BigPond Cable, select this option and fill in the Login Server and Idle Timeout fields. The Login Server is the IP address of the local BigPond Login Server in your area. You can find login server information at <http://www.netgear.com.sg/support/bigpond.asp>
3. If your ISP has assigned a fixed (static or permanent) IP address, select the **Use Static IP Address** radio box and fill in the following fields:
- a. **IP Address:** Static IP address assigned to you. This will identify the router to your ISP.
 - b. **Subnet Mask:** This is usually provided by the ISP or your network administrator.
 - c. **Gateway IP Address:** IP address of the ISP’s gateway. This is usually provided by the ISP or your network administrator.

If your ISP has not assigned a Static IP address, select the **Get dynamically from ISP** radio box. The ISP will automatically assign an IP address to the router using DHCP network protocol.

4. If your ISP has not assigned any Domain Name Servers (DNS) addresses, select the **Get dynamically from ISP** radio box. If your ISP has assigned DNS addresses, select the **Use these DNS Servers** radio box. Ensure that you fill in valid DNS server IP addresses in the fields. Incorrect DNS entries may cause connectivity issues.



Note: Domain Name Servers (DNS) convert Internet names such as www.google.com, www.netgear.com, etc. to Internet addresses called IP addresses. Incorrect settings here will result in connectivity problems.

5. Click **Apply** to save the settings.
6. Click **Reset** to discard any changes and revert to the previous settings.
7. Click **Test** to try and connect to the NETGEAR Web site. If you connect successfully and your settings work, then you may click Logout or go on and configure additional settings.

To configure your WAN2 ISP settings:

1. Select the **WAN2 ISP Settings** tab. The **WAN2 ISP Settings** screen will display.
2. Repeat steps 1 through 7 above.

Programming the Traffic Meter (if Desired)

The traffic meter is useful when an ISP charges by traffic volume over a given period of time or if you want to look at traffic types over a period of time.

To enable the traffic meter:

1. From the primary menu, select **Monitoring**, and then select **Traffic Meter** from the secondary menu. The **WAN1 Traffic Meter** screen will display. Fill out the information described in [Table 2-2](#).

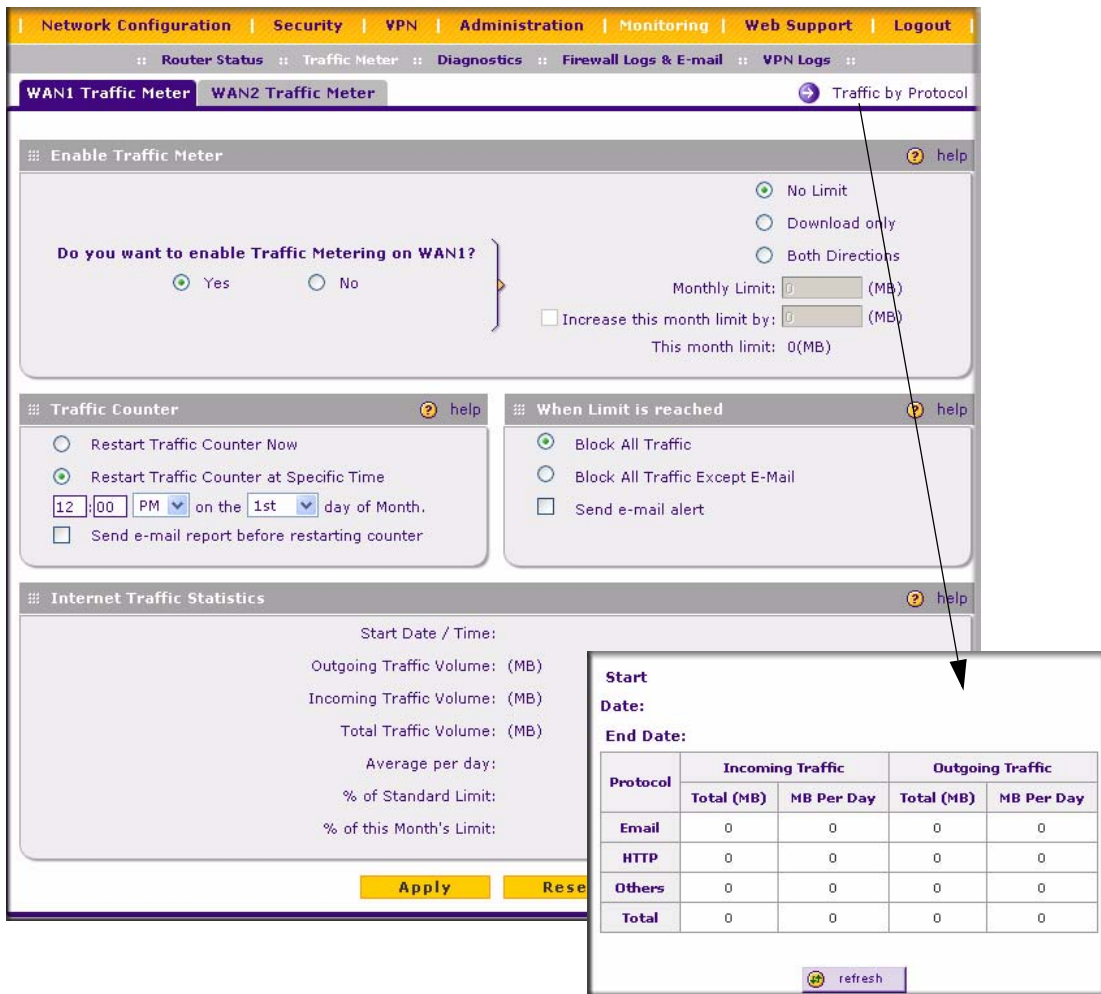


Figure 2-3

2. Click **Apply** to apply the settings. Click **Reset** to return to the previous settings.
3. Select the **WAN2 Traffic Meter** tab and repeat steps 1 through 3 to set the Traffic Meter the the WAN2 port.

Table 2-2. Traffic Meter Settings

Parameter	Description
Enable Traffic Meter	<p>Check this if you wish to record the volume of Internet traffic passing through the Router's WAN1 or WAN2 port. WAN1 or WAN2 can be selected by clicking the appropriate tab; the entire configuration is specific to each wan interface.</p> <ul style="list-style-type: none"> • No Limit - If this is selected specified restriction will not be applied when traffic limit is reached. • Download only - If this is selected the specified restriction will be applied to the incoming traffic only • Both Directions - If this is selected the specified restriction will be applied to both incoming and outgoing traffic only
Enable Monthly Limit	<p>Use this if your ISP charges for additional traffic. If enabled, enter the monthly volume limit and select the desired behavior when the limit is reached.</p> <p>Note: Both incoming and outgoing traffic are included in the limit.</p>
Increase this month's limit	<p>Use this to temporarily increase the Traffic Limit if you have reached the monthly limit, but need to continue accessing the Internet. Check the checkbox and enter the desired increase. (The checkbox will automatically be cleared when saved so the increase is only applied once.)</p>
This month's limit	<p>This displays the limit for the current month.</p>
Restart traffic counter	<p>This determines when the traffic counter restarts. Choose the desired time and day of the month.</p>
Restart Counter at a Specific Time	<p>Check this radio button to restart the Traffic Counter at a specific time and day of the month. Fill in the time fields and select AM or PM and the day of the month from the pull-down menus.</p>
Send E-mail Report before restarting counter	<p>If checked, an E-mail report will be sent immediately before restarting the counter. You must configure the E-mail screen in order for this function to work (see "E-Mail Notifications of Event Logs and Alerts" on page 4-31).</p>
When limit is reached	<p>Select the desired option:</p> <ul style="list-style-type: none"> • Block all traffic - all access to and from the Internet will be blocked. • Block all traffic except E-mail - Only E-mail traffic will be allowed. All other traffic will be blocked. • If using this option, you may also select the Send E-mail alert option. You must configure the E-mail screen in order for this function to work.
Internet Traffic Statistics	<p>This displays statistics on Internet Traffic via the WAN port. If you have not enabled the Traffic Meter, these statistics are not available.</p>
Traffic by Protocol	<p>Click this link if you want to know more details of the Internet Traffic. The volume of traffic for each protocol will be displayed in a sub-window. Traffic counters are updated in MBytes scale, counter starts only when traffic passed is at least 1MB.</p>

Configuring the WAN Mode (Required for Dual WAN)

The dual WAN ports of the ProSafe VPN Firewall 200 can be configured on a mutually exclusive basis for either auto-rollover (for increased system reliability) or load balancing (for maximum bandwidth efficiency).

- **Auto-Rollover Mode.** In this mode, the selected WAN interface is made primary and the other is the rollover link. As long as the primary link is up, all traffic is sent over the primary link. Once the primary WAN interface goes down, the rollover link is brought up to send the traffic. Traffic will automatically roll back to the original primary link once the original primary link is back up and running again.

If you want to use a redundant ISP link for backup purposes, select the WAN port that will act as the primary link for this mode. Ensure that the backup WAN port has also been configured and that you configure the **WAN Failure Detection Method** to support Auto-Rollover.

- **Load Balancing Mode.** In this mode the router distributes the outbound traffic equally among the WAN interfaces that are functional.



Note: Scenarios could arise when load balancing needs to be bypassed for certain traffic or applications. Here the traffic needs to go on a specific WAN interface. This is done with the protocol binding rules of that WAN interface. The rule should match the desired traffic.

For both alternatives, you must also set up Network Address Translation (NAT):

- **NAT.** NAT is the technology which allows all PCs on your LAN to share a single Internet IP address. From the Internet, there is only a single device (the Router) and a single IP address. PCs on your LAN can use any private IP address range, and these IP addresses are not visible from the Internet.
 - The Router uses NAT to select the correct PC (on your LAN) to receive any incoming data.
 - If you only have a single Internet IP address, you **MUST** use NAT.

NAT is the default setting.

- **Classical Routing.** In this mode, the Router performs Routing, but without NAT. To gain Internet access, each PC on your LAN must have a valid Internet IP address.

If your ISP has allocated many IP addresses to you, and you have assigned one of these addresses to each PC, you can choose Classical Routing. Or, you can use Classical Routing for routing private IP addresses within a campus environment. Otherwise, selecting this method will not allow Internet access through this Router.

To learn the status of the WAN ports, you can view the Router Status page (see [“Viewing Router Configuration and System Status” on page 6-23](#)) or look at the LEDs on the front panel (see [“Router Front Panel” on page 1-6](#)).

Setting Up Auto-Rollover Mode

If you want to use a redundant ISP link for backup purposes, ensure that the backup WAN port has already been configured. Then you select the WAN port that will act as the primary link for this mode and configure the **WAN Failure Detection Method** to support Auto-Rollover.

When the router is configured in Auto-Rollover Mode, the router uses the **WAN Failure Detection Method** to check the connection of the primary link at regular intervals to detect router status. Link failure is detected in one of the following ways:

- By using DNS queries to a DNS server, or
- By a Ping to an IP address.

For each WAN interface, DNS queries or Ping requests are sent to the specified IP address. If replies are not received, the corresponding WAN interface is considered down.

To configure the dual WAN ports for Auto-Rollover

1. Select **Network Configuration** from the primary menu and **WAN Mode** from the secondary menu. The WAN Mode screen will display.
2. In the **Port Mode** section, check the **Auto-Rollover Using WAN port** radio box.
3. Selection the WAN port that will act as the primary link for this mode from the pull-down menu.
4. From the **WAN Failure detection Method** section, select the detection failure method radio box from one of the following choices:
 - **DNS lookup using configured DNS Servers (ISP DNS Servers)** – In this case, DNS queries are sent to the DNS server configured on the WAN ISP pages (see [“Configuring the Internet Connections to Your ISPs” on page 2-2](#)).
 - **DNS lookup using this DNS Server** (for example, a public DNS Server) – Enter any public DNS server. DNS queries are sent to this server through the WAN interface being monitored.

- **Ping to this IP address** – Enter a public IP address that will not reject the Ping request or will not consider the traffic abuse. Queries are sent to this server through the WAN interface being monitored.
5. Enter a **Test Period** in seconds. DNS query is sent periodically after every test period. The default test period is 30 seconds.

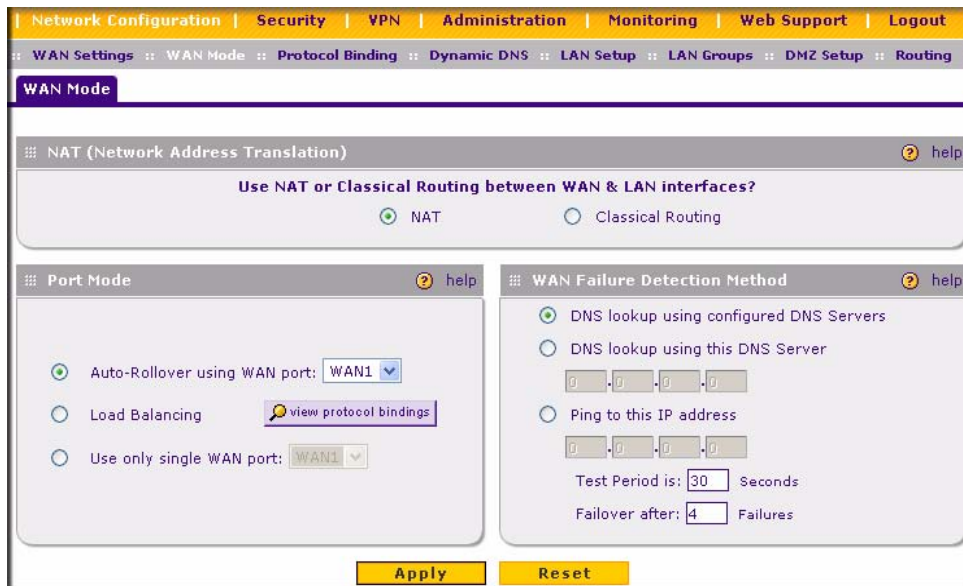


Figure 2-4

6. Enter the **Maximum Failover** amount. The WAN interface is considered down after the configured number of queries have failed to elicit a reply. The rollover link is brought up after this. The Failover default is 4 failures.

The default time to roll over after the primary WAN interface fails is 2 minutes (a 30-second minimum test period, times a minimum of 4 tests).

7. Click **Apply** to save your settings.
8. Click **Reset** to revert to the previous settings.

Once a rollover occurs, an alert will be generated (see [“E-Mail Notifications of Event Logs and Alerts”](#) on page 4-31). When notified that the failed WAN interface has been restored, you can force traffic back on the original primary WAN interface by reapplying the Auto-Rollover settings in the WAN Port Mode menu.

Setting Up Load Balancing

To use multiple ISP links simultaneously, select Load Balancing. In Load Balancing mode, both links will carry data for the protocols that are bound to them. For example, if the HTTP protocol is bound to WAN1 and the FTP protocol is bound to WAN2, then the router will automatically channel FTP data from and to the computers on the LAN through the WAN2 port. All HTTP traffic will be routed through the WAN1 port.

Load Balancing can be used to segregate traffic between links that are not of the same speed. High volume traffic can be routed through the port connected to a high speed link and low volume traffic can be routed through the port connected to the low speed link.

To configure the dual WAN ports for load balancing with protocol binding:

1. Check the Load Balancing radio button on the WAN Mode screen shown in [Figure 2-4](#) above, and click **view protocol bindings** (if protocol binding is needed). The **WAN1 Protocol Bindings** screen will display.

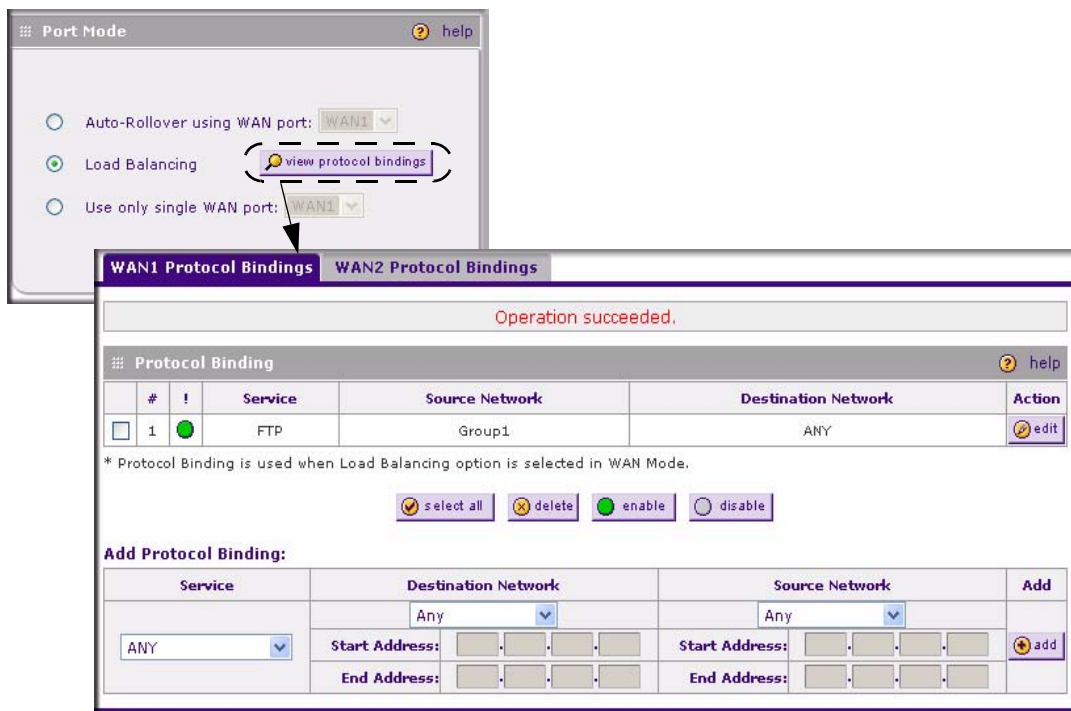


Figure 2-5

2. Enter the following data in the **Add Protocol Binding** section:

- a. **Service** – From the pull-down menu, select the desired Services or applications to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see “[Services-Based Rules](#)” on page 4-2).
 - b. **Destination Network** – These settings determine which Internet locations are covered by the rule, based on their IP address. Select the desired option:
 - **Any** – All Internet IP address are covered by this rule.
 - **Single address** – Enter the required address in the start fields.
 - **Address range** – If this option is selected, you must enter the start and finish fields.
 - c. **Source Network** – These settings determine which computers on your network are affected by this rule. Select the desired options:
 - **Any** – All PCs and devices on your LAN.
 - **Single address** – Enter the required address and the rule will be applied to that particular PC.
 - **Address range** – If this option is selected, you must enter the start and finish fields.
 - **Group 1-Group 8** – If this option is selected, the devices assigned to this group will be affected. (You may also assign a customized name to the group. See **Edit Group Names** on the **Groups and Hosts** menu in the **LAN Groups** sub-menu.)
3. Click **Add** in the Add column adjacent to the rule. The new Protocol Binding Rule will be enabled and added to the Protocol Binding Table for the WAN1 port.

Select the **WAN2 Protocol Bindings** tab, and repeat steps 1 through 9, to set protocol bindings for the WAN2 port.

To Edit or Add additional Protocol Binding settings:

1. Select **Network Configuration** from the main menu and **Protocol Binding** from the submenu. The **WAN1 Protocol Bindings** screen will display.

You can add or edit protocol bindings to either the WAN1 port or click the **WAN2 Protocol Bindings** tab to access the **WAN2 Protocol Bindings** screen. To add a new protocol binding, following the preceding procedure.

2. Check the radio button adjacent to the protocol binding rule you want to modify. Click **Edit** in the Action column adjacent to the rule. The **Edit Protocol Binding** screen will display.

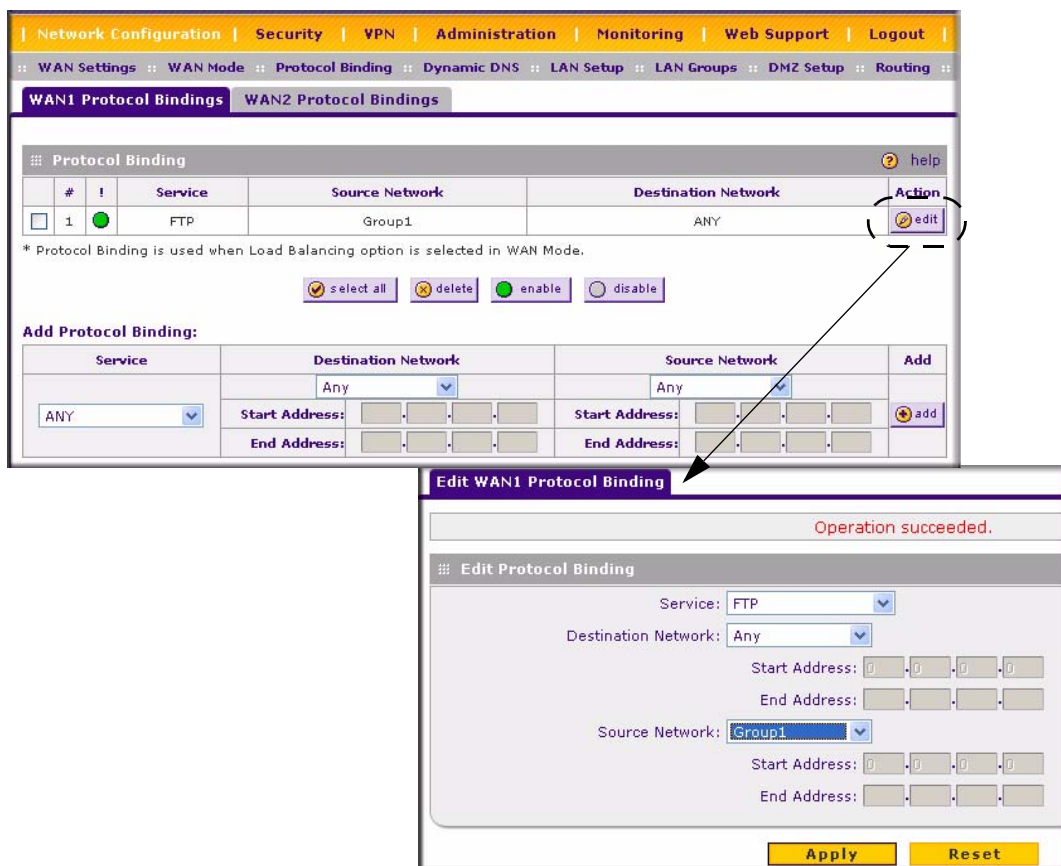


Figure 2-6

3. Modify the parameters for the protocol binding service you selected.
4. Click **Apply**. The modified rule will be enabled and appear in the Protocol Binding table.
5. Click **Reset** to return to the previously configured settings.

Configuring Dynamic DNS (If Needed)

Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. To use DDNS, you must setup an account with a DDNS provider such as DynDNS.org, TZO.com or Iego.net. (Links to DynDNS, TZO and Iego

are provided for your convenience on the **Dynamic DNS Configuration** screen.) The VPN firewall firmware includes software that notifies dynamic DNS servers of changes in the WAN IP address, so that the services running on this network can be accessed by others on the Internet.

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently—hence, the need for a commercial DDNS service, which allows you to register an extension to its domain, and restores DNS requests for the resulting FQDN to your frequently-changing IP address.

After you have configured your account information in the firewall, whenever your ISP-assigned IP address changes, your firewall will automatically contact your DDNS service provider, log in to your account, and register your new IP address.

- For auto-rollover mode, you will need a fully qualified domain name (FQDN) to implement features such as exposed hosts and virtual private networks regardless of whether you have a fixed or dynamic IP address.
- For load balancing mode, you may still need a fully qualified domain name (FQDN) either for convenience or if you have a dynamic IP address.



Note: If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the dynamic DNS service will not work because private addresses will not be routed on the Internet.

To configure Dynamic DNS:

1. Select **Network Configuration** from the primary menu and **Dynamic DNS** from the sub-menu. The **Dynamic DNS Configuration** screen will display.

The **WAN Mode** section displays the currently configured WAN mode (for example, Single Port WAN1, Load Balancing or Auto Rollover). Only those options that match the configured WAN Mode will be accessible.

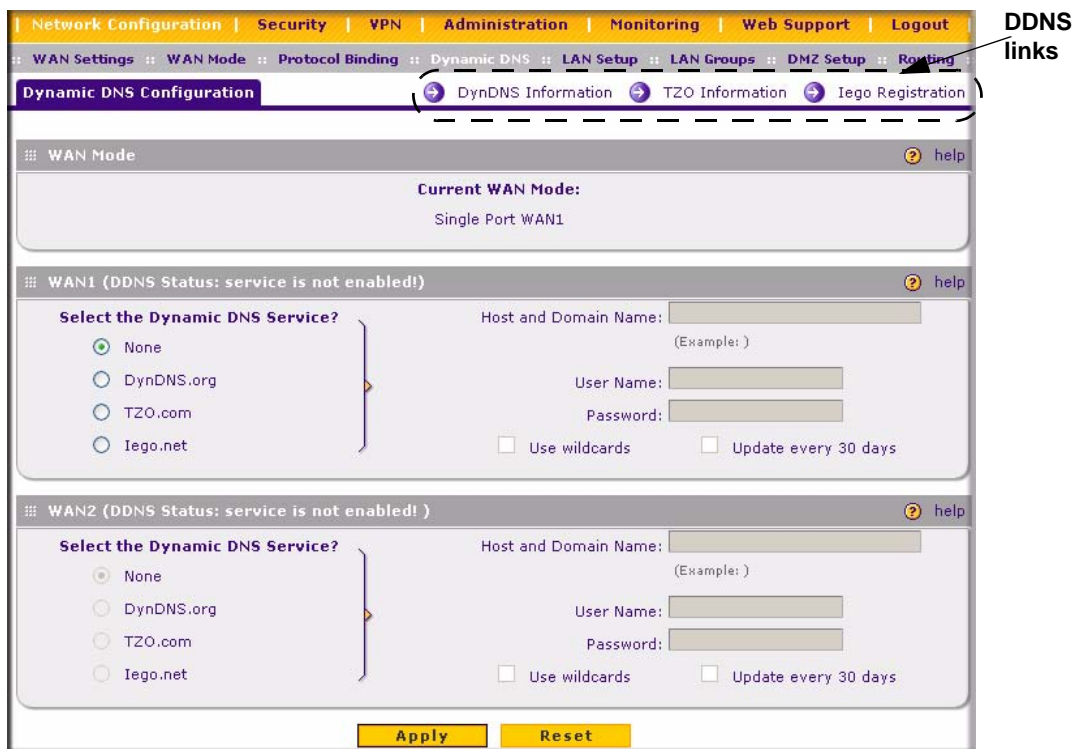


Figure 2-7

2. Check the Dynamic DNS Service radio box you want to enable. The fields corresponding to the selection you have chosen will be highlighted. Each DNS service provider requires its own parameters.
3. Access the Web site of one of the DDNS service providers and set up an account. A link to each DDNS provider is opposite the DNS Configuration screen name.
4. After setting up your account, return to the **Dynamic DNS Configuration** screen and fill in the required fields for the DDNS service you selected:
 - a. In the Host and Domain Name field, enter the entire FQDN name that your dynamic DNS service provider gave you (for example: <yourname>.dyndns.org).
 - b. Enter the User Name, User email Address, or Account Name requested by the DDNS Service to identify you when logging into your DDNS account.
 - c. Enter the Password, or User Key, for your DDNS account.

- d. If your dynamic DNS provider allows the use of wild cards in resolving your URL, you may check the **Use wildcards** radio box to activate this feature.

For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org

5. Click **Apply** to save your configuration.
6. Click **Reset** to return to the previous settings.

Configuring the Advanced WAN Options (If Needed)

To configure the Advanced WAN options:

1. If you haven't already, log in to the firewall at the default LAN address of **http://192.168.1.1**, default user name of **admin**, and default password of **password** (or whatever password and LAN address you have chosen for the firewall).
2. Select **Network Configuration** from the primary menu and **WAN Settings** from the sub-menu. The **WAN Settings** screen will display. Click **Advanced** to access the **WAN1 Advanced Options** screen.

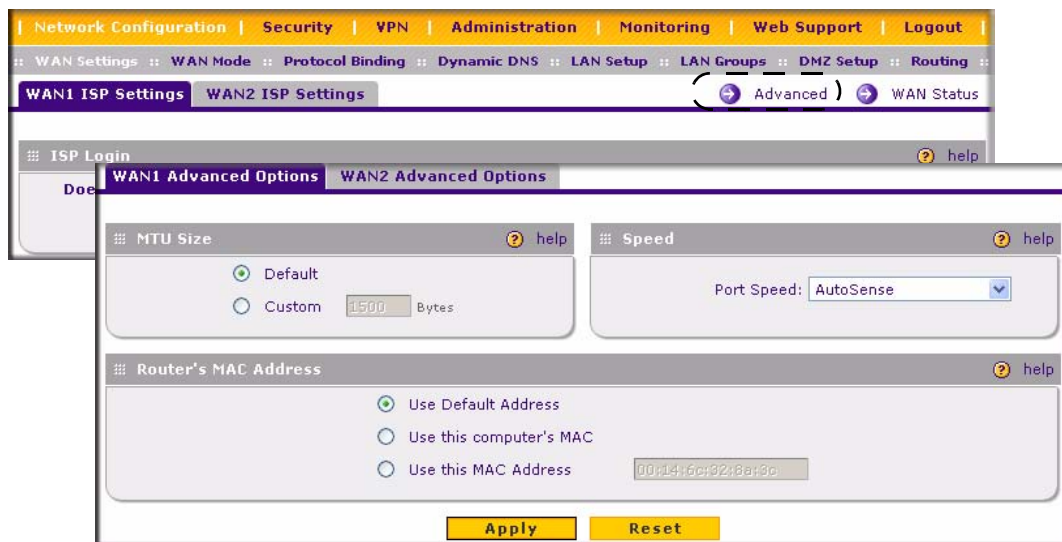


Figure 2-8

3. Edit the default information you want to change.

- **MTU Size** – The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes, or 1492 Bytes for PPPoE connections. For some ISPs you may have to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Port Speed** – In most cases, your router can automatically determine the connection speed of the Internet (WAN) port. If you cannot establish an Internet connection and the Internet LED blinks continuously, you may have to manually select the port speed. AutoSense is the default.

If you know that the Ethernet port on your broadband modem supports 100BaseT, select 100M; otherwise, select 10M. Use the half-duplex settings unless you are sure you need full duplex.

- **Router's MAC Address** – Each computer or router on your network has a unique 32-bit local Ethernet address. This is also referred to as the computer's MAC (Media Access Control) address. The default is **Use default address**. However, if your ISP requires MAC authentication, then select either
 - Use this Computer's MAC address to have the router use the MAC address of the computer you are now using, or
 - Use This MAC Address to manually type in the MAC address that your ISP expects.

The format for the MAC address is XX:XX:XX:XX:XX:XX (numbers 0-9 and either uppercase or lowercase letters A-F). If you select **Use This MAC Address** and then type in a MAC address, your entry will be overwritten.

Chapter 3

LAN Configuration

This chapter describes how to configure the advanced LAN features of your ProSafe VPN Firewall 200. These features can be found by selecting Network Configuration from the primary menu and LAN Setup from the submenu of the browser interface.

Using the Firewall as a DHCP server

By default, the firewall will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, WINS Server, and default gateway addresses to all computers connected to the firewall LAN. The assigned default gateway address is the LAN address of the firewall. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the firewall are satisfactory. See the link to “Preparing a Computer for Network Access” in [Appendix B, “Related Documents”](#) for an explanation of DHCP and information about how to assign IP addresses for your network.

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the **Enable DHCP server** radio box by selecting the **Disable DHCP Server** radio box. Otherwise, leave it checked.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the firewall’s LAN IP address. Using the default addressing scheme, you should define a range between 192.168.1.2 and 192.168.1.100, although you may wish to save part of the range for devices with fixed addresses.

The firewall will deliver the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined.
- Subnet Mask.
- Gateway IP Address (the firewall’s LAN IP address).
- Primary DNS Server (the firewall’s LAN IP address).
- WINS Server (if you entered a WINS server address in the DHCP Setup menu).
- Lease Time (date obtained and duration of lease).

Configuring the LAN Setup Options

The **LAN IP Setup** menu allows configuration of LAN IP services such as DHCP and allows you to configure a secondary or “multi-home” LAN IP setup in the LAN. The default values are suitable for most users and situations. These are advanced settings most usually configured by a network administrator.

To modify your LAN setup:

1. Select **Network Configuration** from the primary menu and **LAN Setup** from the submenu. The **LAN Setup** screen will display.

The screenshot shows the LAN Setup configuration interface. At the top, there is a navigation bar with tabs for Network Configuration, Security, VPN, Administration, Monitoring, Web Support, and Logout. Below this is a breadcrumb trail: WAN Settings :: WAN Mode :: Protocol Binding :: Dynamic DNS :: LAN Setup :: LAN Groups :: DMZ Setup :: Routing. The main title is 'LAN Setup' with sub-links for 'Multi Home LAN IPs Setup' and 'DHCP Log'. The interface is divided into two main sections: 'LAN TCP/IP Setup' and 'DHCP'. The 'LAN TCP/IP Setup' section contains two input fields: 'IP Address' with the value '192.168.1.1' and 'Subnet Mask' with the value '255.255.255.0'. The 'DHCP' section has two radio buttons: 'Disable DHCP Server' (unselected) and 'Enable DHCP Server' (selected). Below these are several input fields: 'Domain Name' (netgear.com), 'Starting IP Address' (192.168.1.2), 'Ending IP Address' (192.168.1.100), 'WINS Server' (empty), 'Lease Time' (24 Hours), and 'Enable DNS Proxy' (checked). At the bottom of the form are two buttons: 'Apply' and 'Reset'.

Figure 3-1

2. Enter the **IP Address** of your router (factory default: **192.168.1.1**). (Always make sure that the LAN Port IP address and DMZ port IP address are in different subnets.)
3. Enter the **IP Subnet Mask**. The subnet mask specifies the network number portion of an IP address. Your router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask (computed by the router).

4. Check the **Enable DHCP Server** radio button. By default, the router will function as a DHCP (Dynamic Host Configuration Protocol) server, providing TCP/IP configuration for all computers connected to the router's LAN. If another device on your network will be the DHCP server, or if you will manually configure all devices, check the **Disable DHCP Server** radio button. Enable DHCP Server is the default. If Enabled is selected, enter the following parameters:
 - a. Enter the **Domain Name** of the router (this is optional).
 - b. Enter the **Starting IP Address**. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN will be assigned an IP address between this address and the Ending IP Address. The IP address 192.168.1.2 is the default start address.
 - c. Enter the **Ending IP Address**. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN will be assigned an IP address between the Starting IP address and this IP address. The IP address 192.168.1.100 is the default ending address.



Note: The Starting and Ending DHCP addresses should be in the same “network” as the LAN TCP/IP address of the router (the IP Address in **LAN TCP/IP Setup** section).

- d. Enter a **WINS Server** IP address. This box can specify the Windows NetBios Server IP if one is present in your network. This field is optional.
- e. Enter a **Lease Time**. This specifies the duration for which IP addresses will be leased to clients.
- f. Check the **Enable DNS Proxy** radio box. This is optional—the default is enabled. If enabled, the VPN firewall will provide a LAN IP Address for DNS address name resolution.



Note: If you change the LAN IP address of the firewall while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again. For example, if you change the default IP address 192.168.1.1 to 10.0.0.1, you must enter **http://10.0.0.1** in your browser to reconnect to the web management interface.

5. Click **Apply** to save your settings.

6. Click **Reset** to discard any changes and revert to the previous configuration.



Note: Once you have completed the LAN IP setup, all outbound traffic is allowed and all inbound traffic is discarded. To change these traffic rules, refer to [Chapter 4, “Firewall Protection and Content Filtering.”](#)

Configuring Multi Home LAN IPs

If you have computers on your LAN using different IP address ranges (for example, 172.16.2.0 or 10.0.0.0), then you can add “aliases” to the LAN port thereby giving computers on those networks access to the Internet. This allows the firewall to act as a gateway to additional logical subnets on your LAN. You can assign the firewall an IP address on each additional logical subnet

- The **Available Secondary LAN IPs** table lists the secondary LAN IP addresses added to the router.
- The **IP Address** is the “alias” added to the LAN port of the router. This will be the gateway for computers that need to access the Internet.
- The **Subnet Mask** is the IPv4 Subnet Mask.

To add a secondary LAN IP address:

1. Enter the IP Address and the Subnet Mask in the respective fields of the **Add Secondary LAN IP Address** section.
2. Click **Add**. The new Secondary LAN IP address will appear in the **Available Secondary LAN IPs** table.
3. Click **Select all** to select all the entries in the **Available Secondary LAN IPs** table. All the radio buttons are selected.
4. Click **Delete** to delete only those entries with checked radio buttons from the Available Secondary LAN IPs table.

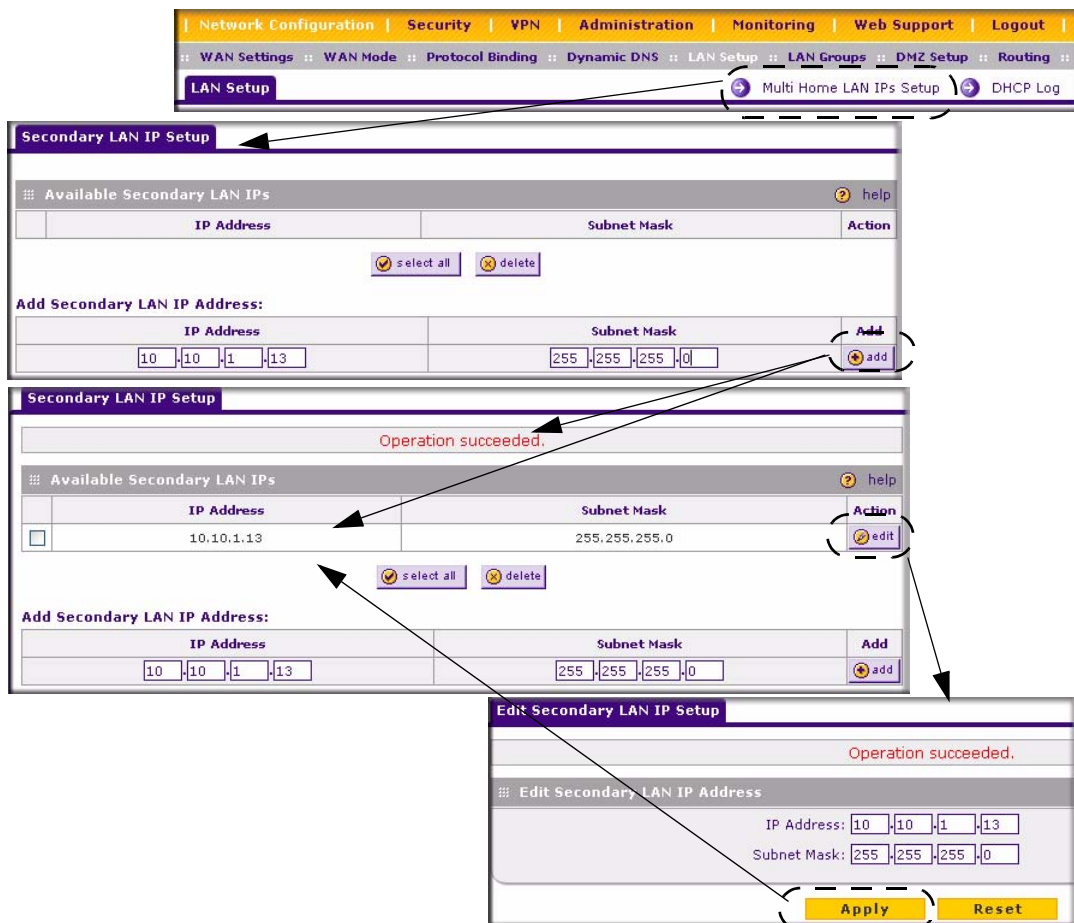



Figure 3-2

 **Note:** Additional IP addresses cannot be configured in the DHCP server. The hosts on the secondary subnets must be manually configured with IP addresses, gateway IP and DNS server IPs.

To make changes to the selected entry:

1. Click **Edit** in the Action column adjacent to the selected entry. The **Edit Secondary LAN IP Setup** screen will display.
2. Modify the **IP Address** and **Subnet Mask** fields and click **Apply**.

3. Click **Reset** to discard any changes and revert to the previous settings.



Tip: The Secondary LAN IP address will be assigned to the LAN interface of the router and can be used as a gateway by the secondary subnet.

Managing Groups and Hosts (LAN Groups)

The **Known PCs and Devices** table on the **Groups and Hosts** screen contains a list of all known PCs and network devices, as well as hosts, that are assigned dynamic IP addresses by this router. Collectively, these entries make up the Network Database. The Network Database is created in two ways:

- **DHCP Client Requests.** By default, the DHCP server in this Router is enabled, and will accept and respond to DHCP client requests from PCs and other network devices. These requests also generate an entry in the Network Database. Because of this, leaving the DHCP Server feature (on the LAN screen) enabled is strongly recommended.
- **Scanning the Network.** The local network is scanned using standard methods such as ARP. This will detect active devices which are not DHCP clients. However, sometimes the name of the PC or device cannot be accurately determined, and will be shown as Unknown.

Creating the Network Database

Some advantages of the Network Database are:

- Generally, you do not need to enter either IP address or MAC addresses. Instead, you can just select the desired PC or device.
- No need to reserve an IP address for a PC in the DHCP Server. All IP address assignments made by the DHCP Server will be maintained until the PC or device is removed from the database, either by expiry (inactive for a long time) or by you.
- No need to use a Fixed IP on PCs. Because the address allocated by the DHCP Server will never change, you don't need to assign a fixed IP to a PC to ensure it always has the same IP address.
- MAC level control over PCs. The Network Database uses the MAC address to identify each PC or device. So changing a PC's IP address does not affect any restrictions on that PC.
- Group and individual control over PCs.

- You can assign PCs to Groups and apply restrictions to each Group using the Firewall Rules screen (see [“Using Rules to Block or Allow Specific Kinds of Traffic”](#) on page 4-1).
 - You can also select the Groups to be covered by the Block Sites feature (see [“Setting Block Sites \(Content Filtering\)”](#) on page 4-25).
 - If necessary, you can also create Firewall Rules to apply to a single PC (see [“Enabling Source MAC Filtering”](#) on page 4-27). Because the MAC address is used to identify each PC, users cannot avoid these restrictions by changing their IP address.
- A computer is identified by its MAC address—not its IP address. Hence, changing a computer’s IP address does not affect any restrictions applied to that PC.

This **Known PCs and Devices** table lists entries in the Network Database. For each computer or device, the following fields are displayed:

- **Name:** The name of the PC or device. For computers that do not support the NetBIOS protocol, this will be listed as “Unknown” (you can edit the entry manually to add a meaningful name). If the computer was assigned an IP address by the DHCP server, then the Name will be appended by an asterisk.
- **IP Address:** The current IP address of the computer. For DHCP clients of the router, this IP address will not change. If a computer is assigned a static IP addresses, you will need to update this entry manually if the IP address on the computer has been changed.
- **MAC Address:** The MAC address of the PC’s network interface.
- **Group:** Each PC or device can be assigned to a single group. By default, a computer is assigned to Group 1, unless a different group is selected from the Group pull-down menu.
- **Action:** Allows modification of the selected entry by clicking Edit.

To add computers to the network database manually:

1. Select **Network Configuration** from the main menu and **LAN Groups** from the submenu. The **Groups and Hosts** screen will display.
2. In the **Add Known PCs and Devices** table, enter the name of the PC or device.
3. From the **IP Address Type** pull-down menu, select Reserved (DHCP Client) to direct the router to reserve the IP address for allocation by the DHCP server, or select Fixed (Set on PC) if the IP address is statically assigned on the computer.



Note: When assigning a Reserved IP address to a client, the IP address selected must be outside the range of addresses allocated to the DHCP Server pool.

4. Enter the IP Address that this computer or device is assigned in the **IP Address** field. If the IP Address Type is Reserved (DHCP Client), the router will reserve the IP address for the associated MAC address.
5. Enter the MAC Address of the computer's network interface in the **MAC Address** field. The MAC address should be in the form: xx:xx:xx:xx:xx:xx (for example: 00:80:48:2a:8b:c0 that contain numbers 0-9 and letters a-f).
6. From the **Group** pull-down menu, enter the Group to which the computer will be assigned. (Group 1 is the default group.)
7. Click **Add**. The device will be added to the **Known PCs and Devices** table.

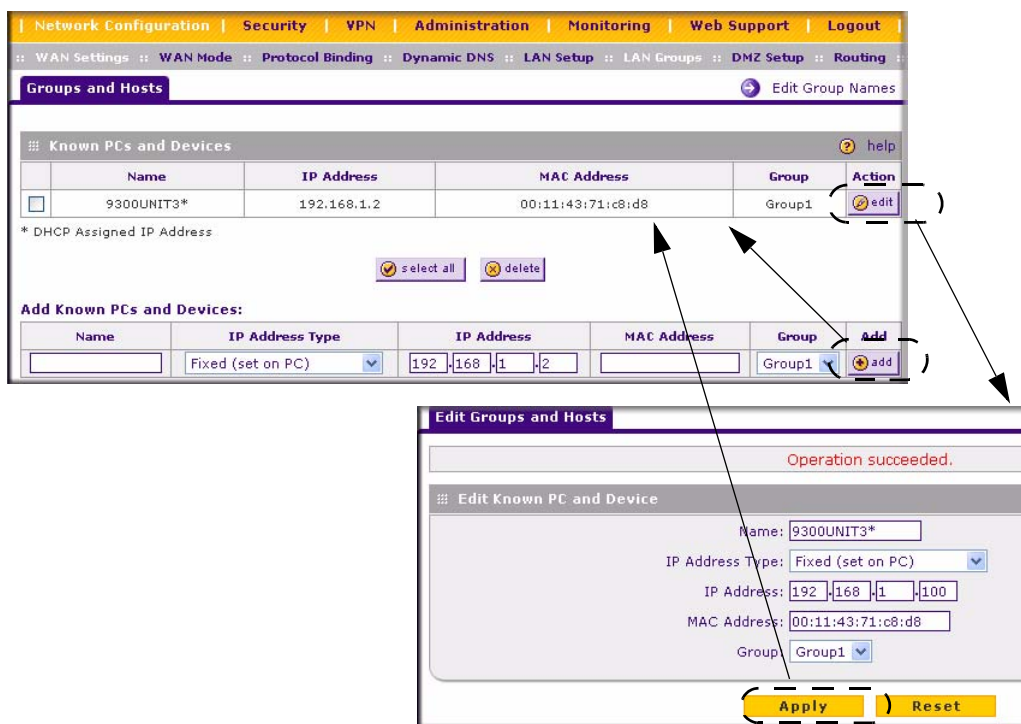


Figure 3-3

To edit the information of any of the Known PCs or Devices:

1. Click **Edit** in the Action column opposite the name of the device. The **Edit Groups and Hosts** screen will display.
2. Modify any of the fields on this screen.
3. Click **Reset** to cancel your settings and return to the previous settings.

4. Click **Apply** to save your new settings. The modified record will appear in the **Known PCs and Devices** table.

To edit the names of any of the eight available groups:

1. Click **Edit Group Names** at the upper right of the **Groups and Hosts** screen. The **Network Database Group Names** screen will display.
2. Check the radio button opposite the Group Name you want to change and type a suitable name in the field.
3. Click **Reset** to discard any changes and revert to the previous settings.
4. Click **Apply** to save the settings.

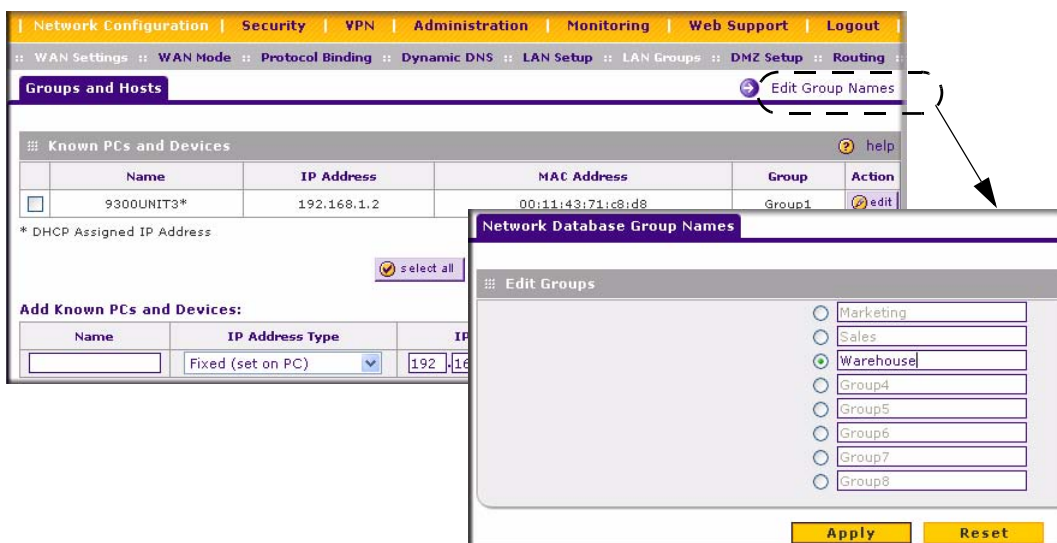


Figure 3-4

Setting Up Address Reservation

When you specify a reserved IP address for a device on the LAN (based on the MAC address of the device), that computer or device will always receive the same IP address each time it accesses the firewall's DHCP server. Reserved IP addresses should be assigned to servers or access points that require permanent IP settings. The Reserved IP address that you select must be outside of the DHCP Server pool.

To reserve an IP address, use the **Groups and Hosts** screen under the **Network Configuration** menu, **LAN Groups** submenu (see [“Creating the Network Database” on page 3-6](#)).



Note: The reserved address will not be assigned until the next time the PC contacts the firewall's DHCP server. Reboot the PC or access its IP configuration and force a DHCP release and renew.

Configuring and Enabling the DMZ Port

The De-Militarized Zone (DMZ) is a network which, when compared to the LAN, has fewer firewall restrictions, by default. This zone can be used to host servers (such as a web server, ftp server, or email server, for example) and give public access to them. The eighth LAN port on the router can be dedicated as a hardware DMZ port for safely providing services to the Internet, without compromising security on your LAN.

The DMZ port feature is also helpful when using some online games and videoconferencing applications that are incompatible with NAT. The firewall is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, local PCs can run the application properly if those PCs are used on the DMZ port.



Note: A separate firewall security profile is provided for the DMZ port that is independent of the standard firewall security used for the LAN.

The **DMZ Setup** screen allows you to set up the DMZ port. It permits you to enable or disable the hardware DMZ port (LAN port 8, see [“Router Front Panel” on page 1-6](#)) and configure an IP address and Mask for the DMZ port.

To enable and configure the DMZ port:

1. From the main menu, select **Network Configuration** and then select **DMZ Setup** from the submenu. The **DMZ Setup** screen will display.
2. Check the **Do you want to enable DMA Port?** radio box.
3. Enter an **IP Address** and the **Subnet mask** for the DMZ port. Make sure that the DMZ port IP address and LAN Port IP address are in different subnets (for example, an address outside the LAN Address pool, such as 192.168.1.101).

Figure 3-5

4. If desired, **Enable the DHCP Server** (Dynamic Host Configuration Protocol), which will provide TCP/IP configuration for all computers connected to the router's DMZ network. Then configure the following items:
 - a. **Starting IP Address** – This box specifies the first of the contiguous addresses in the IP address pool.
 - b. **Ending IP Address** – This box specifies the last of the contiguous addresses in the IP address pool.
 - c. **WINS Server** – This box specifies the Windows Internet Naming Service Server IP.
 - d. **Lease Time** – This box specifies the Lease time to be given to the DHCP Clients.
 - e. **Enable DNS Proxy** – If enabled, the VPN firewall will act as a DNS for address resolution.
5. Click **Reset** to cancel changes made on this screen and revert to the previous settings.
6. Click **Apply** to save your settings. The DMZ LED next to LAN port 8 (see [“Router Front Panel” on page 1-6](#)) will light up indicating that the DMZ port has been enabled.

If another device on your DMZ network will be the DHCP server, or if you will manually configure all devices, leave the Disable option (default) checked.

To define the DMZ WAN Rules and LAN DMZ Rules, see [“Setting DMZ WAN Rules” on page 4-10](#) and [“Setting LAN DMZ Rules” on page 4-12](#), respectively.

Static Routes

Static Routes provide additional routing information to your firewall. Under normal circumstances, the firewall has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You should configure static routes only for unusual cases such as multiple firewalls or multiple IP subnets located on your network.

Configuring Static Routes

To add or edit a static route:

1. Select **Network Configuration** from the main menu and **Routing** from the submenu. The **Routing** screen will display.
2. Click **Add**. The **Add Static Route** menu, shown below, will display.
3. Enter a route name for this static route in the **Route Name** field (for identification and management).

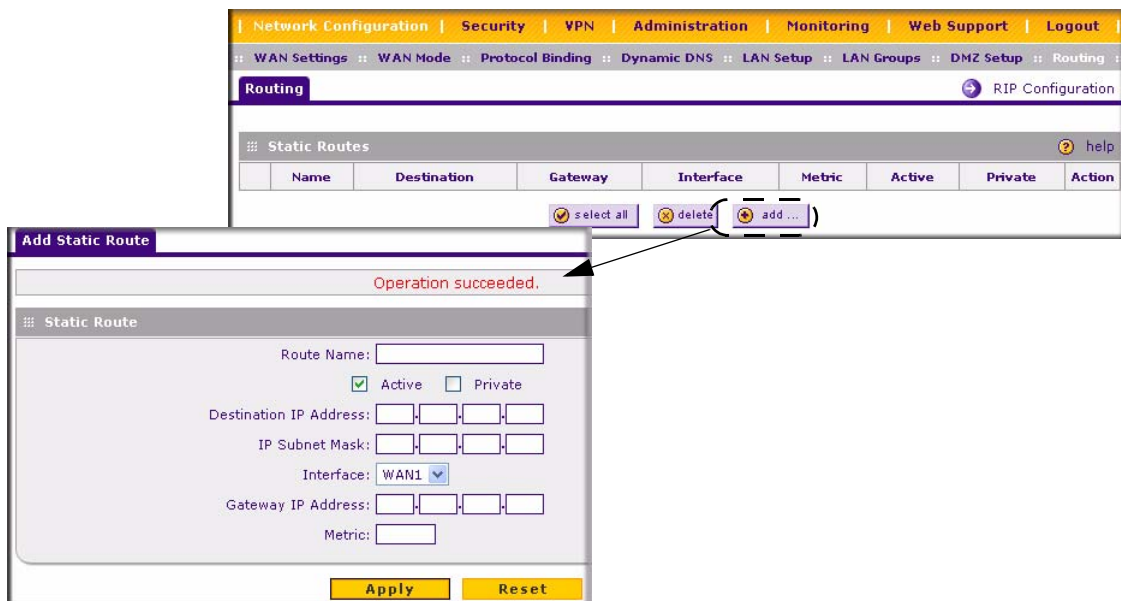


Figure 3-6

4. Select **Active** to make this route effective.
5. Select **Private** if you want to limit access to the LAN only. The static route will not be advertised in RIP.
6. Enter the **Destination IP Address** to the host or network to which the route leads.
7. Enter the **IP Subnet Mask** for this destination. If the destination is a single host, enter 255.255.255.255.
8. Enter the **Interface** which is the physical network interface (WAN1, WAN2, or LAN) through which this route is accessible.
9. Enter the **Gateway IP Address** through which the destination host or network can be reached (must be a firewall on the same LAN segment as the firewall).
10. Enter the **Metric** priority for this route. If multiple routes to the same destination exist, the route with the lowest metric is chosen. (value must be between 1 and 15),
11. Click **Reset** to discard any changes and revert to the previous settings.
12. Click **Apply** to save your settings. The new static route will be added to Route table.

You can edit the route's settings by clicking **Edit** in the Action column adjacent to the route.

Routing Information Protocol (RIP)

RIP (Routing Information Protocol, RFC 2453) is an Interior Gateway Protocol (IGP) that is commonly used in internal networks (LANs). It allows a router to exchange its routing information automatically with other routers, and allows it to dynamically adjust its routing tables and adapt to changes in the network. RIP is disabled by default.

To configure RIP parameters:

1. Select **Network Configuration** from the main menu and **Routing** from the submenu. When the **Routing** screen displays, click **RIP Configuration**. The **RIP Configuration** screen will display.
2. From the **RIP Direction** pull-down menu, select the direction in which the router will send and receives RIP packets. The choices are:
 - **None** – The router neither broadcasts its route table nor does it accept any RIP packets from other routers. This effectively disables RIP.
 - **Both** – The router broadcasts its routing table and also processes RIP information received from other routers.

- **Out Only** – The router broadcasts its routing table periodically but does not accept RIP information from other routers.
- **In Only** – The router accepts RIP information from other routers, but does not broadcast its routing table.

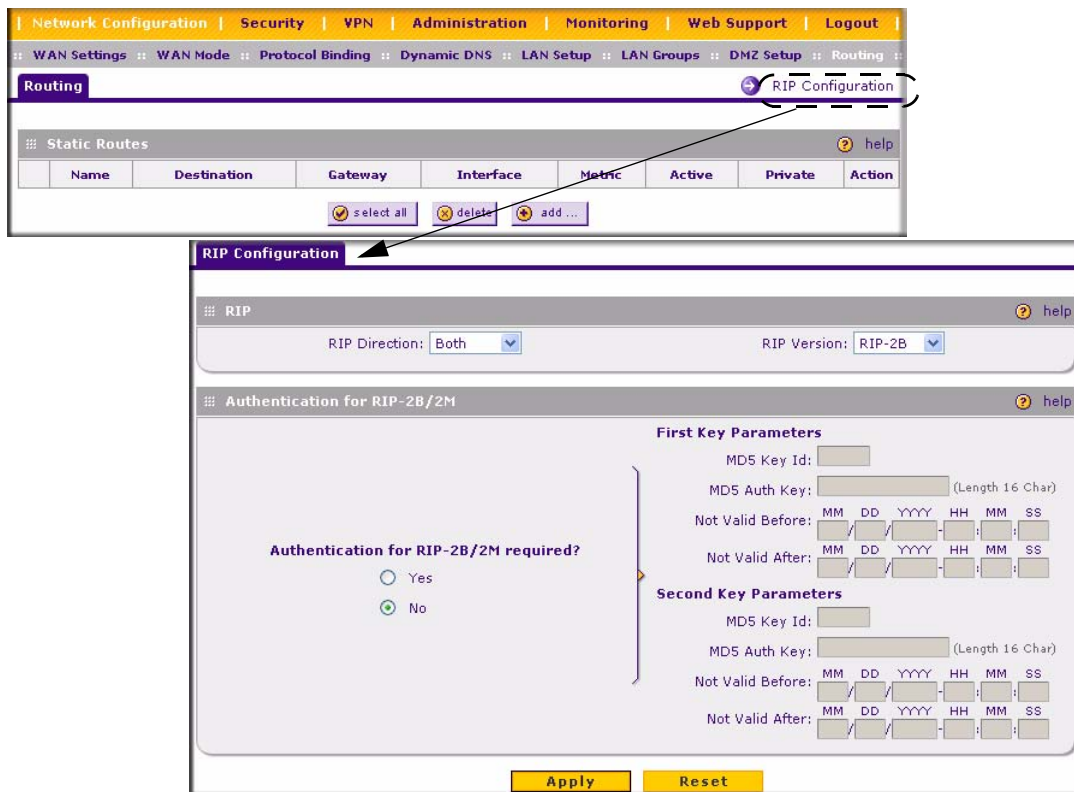


Figure 3-7

3. From the **RIP Version** pull-down menu, select the version:
 - **RIP-1** – A classful routing that does not include subnet information. This is the most commonly supported version.
 - **RIP-2** – Supports subnet information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format:
 - **RIP-2B** Sends the routing data in RIP-2 format and uses subnet broadcasting.
 - **RIP-2M** Sends the routing data in RIP-2 format and uses multicasting.

4. **Authentication for RIP2B/2M required?** If you selected RIP-2B or RIP-2M, check the **YES** radio box to enable the feature, and input the **First Key Parameters** and **Second Key Parameters** MD-5 keys to authenticate between routers.
5. Click **Reset** to discard any changes and revert to the previous settings.
6. Click **Save** to save your settings.

Static Route Example

For example, you may require a static route if:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN firewall on your home network for connecting to the company where you are employed. This firewall's address on your LAN is 192.168.1.100.
- Your company's network is 134.177.0.0.

When you first configured your firewall, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your firewall will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

In this case you must define a static route, telling your firewall that 134.177.0.0 should be accessed through the ISDN firewall at 192.168.1.100.

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN firewall at 192.168.1.100.
- A Metric value of 1 will work since the ISDN firewall is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

Enabling Trend Micro Antivirus Enforcement

If you installed the Trend Micro Client/Server Messaging Suite for SMB on your local network, the firewall can enforce antivirus scanning. When Antivirus Enforcement is selected, local PCs

will not be allowed web access unless they have the Trend Micro OfficeScan client installed and updated with the latest virus definitions.

To enable Trend Micro:

1. Select **Security** from the main menu and **Trend Micro** from the submenu. The **Trend Micro** screen will display.
2. In the **Do you want to enable the Antivirus Enforcement?** section, check the **Yes** radio box.

Figure 3-8

3. Enter the **Office Scan Server IP Address** on the LAN.
4. Then enter the 5-digit port number used for communications between the Office Scan clients and the server in the **Office Scan Client Communication Port**.
5. Finally, enter the **Office Scan Server HTTP Port** (by default port 8080).
6. Click **Apply**.

To allow a PC to access the web without the OfficeScan client:

1. Enter the IP address of a PC to be excluded in the **Add Host** table and then click **Add**. The PC address will appear in the Host Exclusion List table.
2. Add additional PCs, one at a time, until all of the PCs to be excluded are contained in the Host Exclusion List.

3. Click **Apply** to submit your changes.



Note: The Office Scan Server must also appear in the exclusion list!



Note: Follow the instructions in the Trend Micro documentation to complete the installation and configuration of the Trend Micro OfficeScan Server.

Chapter 4

Firewall Protection and Content Filtering

This chapter describes how to use the content filtering features of the ProSafe VPN Firewall 200 to protect your network. These features can be found by selecting **Security** from the main menu and selecting **Block Sites** from the submenu of the browser interface.

About Firewall Protection and Content Filtering

The ProSafe VPN Firewall 200 provides you with Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, Web addresses and Web address keywords. You can also block Internet access by applications and services, such as chat or games.

A firewall is a special category of router that protects one network (the “trusted” network, such as your LAN) from another (the untrusted network, such as the Internet), while allowing communication between the two. You can further segment keyword blocking to certain known groups (see [“Managing Groups and Hosts \(LAN Groups\)”](#) on page 3-6 to set up LAN Groups).

A firewall incorporates the functions of a NAT (Network Address Translation) router, while adding features for dealing with a hacker intrusion or attack, and for controlling the types of traffic that can flow between the two networks. Unlike simple Internet sharing NAT routers, a firewall uses a process called stateful packet inspection to protect your network from attacks and intrusions. NAT performs a very limited stateful inspection in that it considers whether the incoming packet is in response to an outgoing request, but true Stateful Packet Inspection goes far beyond NAT.

Using Rules to Block or Allow Specific Kinds of Traffic

Firewall rules are used to block or allow specific traffic passing through from one side to the other. You can configure up to 600 rules on the FVX538. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the FVX538 are:

- **Inbound:** Block all access from outside except responses to requests from the LAN side.
- **Outbound:** Allow all access from the LAN side to the outside.

The firewall rules for blocking/allowing traffic on the VPN firewall can be applied to LAN/WAN traffic, DMZ/WAN traffic and LAN/DMZ traffic.

Services-Based Rules

The rules to block traffic are based on the traffic's category of service.

- **Outbound Rules (service blocking)** – Outbound traffic is normally allowed unless the firewall is configured to disallow it.
- **Inbound Rules (port forwarding)** – Inbound traffic is normally blocked by the firewall unless the traffic is in response to a request from the LAN side. The firewall can be configured to allow this otherwise blocked traffic.
- **Customized Services** – Additional services can be added to the list of services in the factory default list. These added services can then have rules defined for them to either allow or block that traffic (see [“Adding Customized Services” on page 4-21](#)).
- **Quality of Service (QoS) priorities** – Each service at its own native priority that impacts its quality of performance and tolerance for jitter or delays. You can change this QoS priority if desired to change the traffic mix through the system (see [“Setting Quality of Service \(QoS\) Priorities” on page 4-23](#)).

Outbound Rules (Service Blocking)

The FVX538 allows you to block the use of certain Internet services by PCs on your network. This is called service blocking or port filtering.



Note: See [“Enabling Source MAC Filtering” on page 4-27](#) for yet another way to block outbound traffic from selected PCs that would otherwise be allowed by the firewall.

Table 4-1. Outbound Rules

Item	Description
Service Name	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see “Adding Customized Services” on page 4-21).
Action (Filter)	<p>Select the desired action for outgoing connections covered by this rule:</p> <ul style="list-style-type: none"> • BLOCK always • BLOCK by schedule, otherwise Allow • ALLOW always • ALLOW by schedule, otherwise Block <p>Note: Any outbound traffic which is not blocked by rules you create will be allowed by the Default rule.</p> <p>ALLOW rules are only useful if the traffic is already covered by a BLOCK rule. That is, you wish to allow a subset of traffic that is currently blocked by another rule.</p>
Action (Select Schedule)	<p>Select the desired time schedule (i.e., Schedule1, Schedule2, or Schedule3) that will be used by this rule.</p> <ul style="list-style-type: none"> • This drop down menu gets activated only when “BLOCK by schedule, otherwise Allow” or “ALLOW by schedule, otherwise Block” is selected as Action. • Use schedule page to configure the time schedules (see “Setting a Schedule to Block or Allow Specific Traffic” on page 4-24).
LAN users	<p>These settings determine which computers on your network are affected by this rule. Select the desired options:</p> <ul style="list-style-type: none"> • Any – All PCs and devices on your LAN. • Single address – Enter the required address and the rule will be applied to that particular PC. • Address range – If this option is selected, you must enter the start and finish fields. • Groups – Select the Group to which this rule will apply. Use the LAN Groups screen (under Network Configuration) to assign PCs to Groups. See “Managing Groups and Hosts (LAN Groups)” on page 3-6.
WAN Users	<p>These settings determine which Internet locations are covered by the rule, based on their IP address. Select the desired option:</p> <ul style="list-style-type: none"> • Any – All Internet IP address are covered by this rule. • Single address – Enter the required address in the start field. • Address range – If this option is selected, you must enter the start and end fields.
DMZ Users	<p>These settings determine which DMZ computers on DMZ network are affected by this rule. Select the desired options.</p> <ul style="list-style-type: none"> • Any – All PCs and devices on your DMZ network. • Single address – Enter the required address and the rule will be applied to that particular PC on the DMZ network. • Address range – If this option is selected, you must enter the start and finish fields of the DMZ computers.

Table 4-1. Outbound Rules (continued)

Item	Description
QoS Priority	This setting determines the priority of a service which, in turn, determines the quality of that service for the traffic passing through the firewall. By default, the priority shown is that of the selected service. The user can change it accordingly. If the user does not make a selection (i.e., leaves it as None), then the native priority of the service will be applied to the policy. See “Setting Quality of Service (QoS) Priorities” on page 4-23.
Log	This determines whether packets covered by this rule are logged. Select the desired action: <ul style="list-style-type: none"> • Always – always log traffic considered by this rule, whether it matches or not. This is useful when debugging your rules. • Never – never log traffic considered by this rule, whether it matches or not.

Inbound Rules (Port Forwarding)

Because the FVX538 uses Network Address Translation (NAT), your network presents only one IP address to the Internet and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the firewall to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

Whether or not DHCP is enabled, how the PCs will access the server’s LAN address impacts the Inbound Rules. For example:

- If your external IP address is assigned dynamically by your ISP (DHCP enabled), the IP address may change periodically as the DHCP lease expires. Consider using **Dyamic DNS** (under Network Configuration) so that external users can always find your network (see [“Configuring Dynamic DNS \(If Needed\)” on page 2-15.](#)
- If the IP address of the local server PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, use the Reserved IP address feature in the **LAN Groups** menu (under Network Configuration) to keep the PC’s IP address constant (see [“Setting Up Address Reservation” on page 3-9.](#)
- Local PCs must access the local server using the PCs’ local LAN address. Attempts by local PCs to access the server using the external WAN IP address will fail.



Note: See [“Port Triggering” on page 4-28](#) for yet another way to allow certain types of inbound traffic that would otherwise be blocked by the firewall.

Table 4-2. Inbound Rules

Item	Description
Services	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see “Adding Customized Services” on page 4-21).
Action (Filter)	Select the desired action for packets covered by this rule: <ul style="list-style-type: none"> • BLOCK always • BLOCK by schedule, otherwise Allow • ALLOW always • ALLOW by schedule, otherwise Block Note: Any inbound traffic which is not allowed by rules you create will be blocked by the Default rule.
Action (Select Schedule)	Select the desired time schedule (i.e., Schedule1, Schedule2, or Schedule3) that will be used by this rule (see “Setting a Schedule to Block or Allow Specific Traffic” on page 4-24). <ul style="list-style-type: none"> • This drop down menu gets activated only when “BLOCK by schedule, otherwise Allow” or “ALLOW by schedule, otherwise Block” is selected as Action. • Use schedule page to configure the time schedules.
LAN Server or DMZ Server	This LAN address or DMZ Server address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.)
Translate to Port Number	Check the “Translate to Port Number” and enter a port number if you want to assign the LAN Server to a specific port.
WAN Users	These settings determine which Internet locations are covered by the rule, based on their IP addresses. Select the desired option: <ul style="list-style-type: none"> • Any – All Internet IP address are covered by this rule. • Single address – Enter the required address in the start field. • Address range – If this option is selected, you must enter the start and end fields.
WAN Destination IP Address	This setting determines the destination IP address applicable to incoming traffic. This is the public IP address that will map to the internal LAN server; it can either be the address of the WAN1 or WAN2 ports or another public IP address.

Table 4-2. Inbound Rules (continued)

Item	Description
QoS Priority	This setting determines the priority of a service, which in turn, determines the quality of that service for the traffic passing through the firewall. By default, the priority shown is that of the selected service. The user can change it accordingly. If the user does not make a selection (i.e., leaves it as None), then the native priority of the service will be applied to the policy. See “Setting Quality of Service (QoS) Priorities” on page 4-23 .
Log	This determines whether packets covered by this rule are logged. Select the desired action: <ul style="list-style-type: none">• Always – Always log traffic considered by this rule, whether it matches or not. This is useful when debugging your rules.• Never – Never log traffic considered by this rule, whether it matches or not.



Note: Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

Remember that allowing inbound services opens holes in your VPN firewall. Only enable those ports that are necessary for your network. It is also advisable to turn on the server application security and invoke the user password or privilege levels, if provided.

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu as the last item in the list, as shown in [Figure 4-1](#):

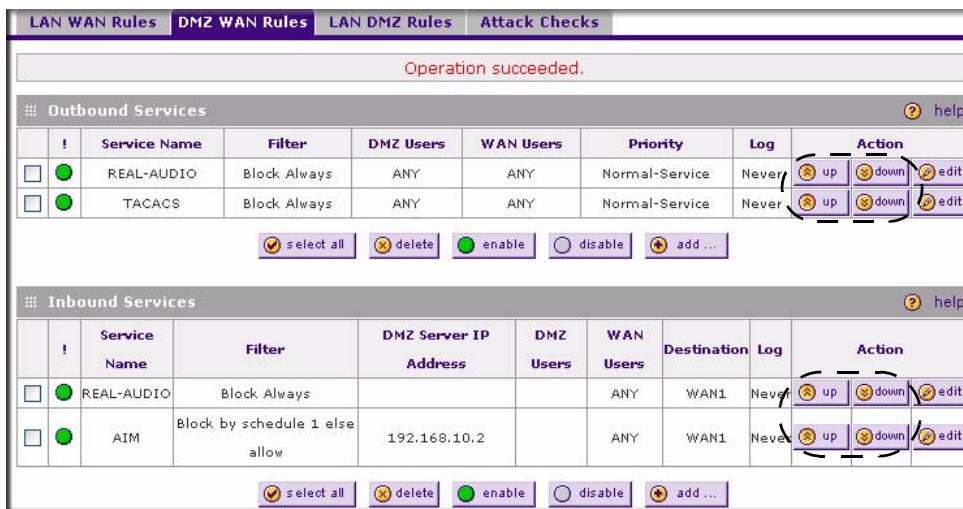


Figure 4-1

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules Table, beginning at the top and proceeding to the bottom. In some cases, the order of precedence of two or more rules may be important in determining the disposition of a packet. For example, you should place the most strict rules at the top (those with the most specific services or addresses). The **Up** and **Down** button allows you to relocate a defined rule to a new position in the table.

Setting LAN WAN Rules

The Default Outbound Policy is to allow all traffic to the Internet to pass through. Firewall rules can then be applied to block specific types of traffic from going out from the LAN to the Internet (Outbound). The default policy of Allow Always can be changed to block all outbound traffic which then allows you to enable only specific services to pass through the router.

To change the Default Outbound Policy:

1. Select **Security** from the main menu and **Firewall Rules** from the submenu. The **LAN WAN Rules** screen will display.

- Change the **Default Outbound Policy** by selecting Block Always from the drop-down menu and click **Apply**..

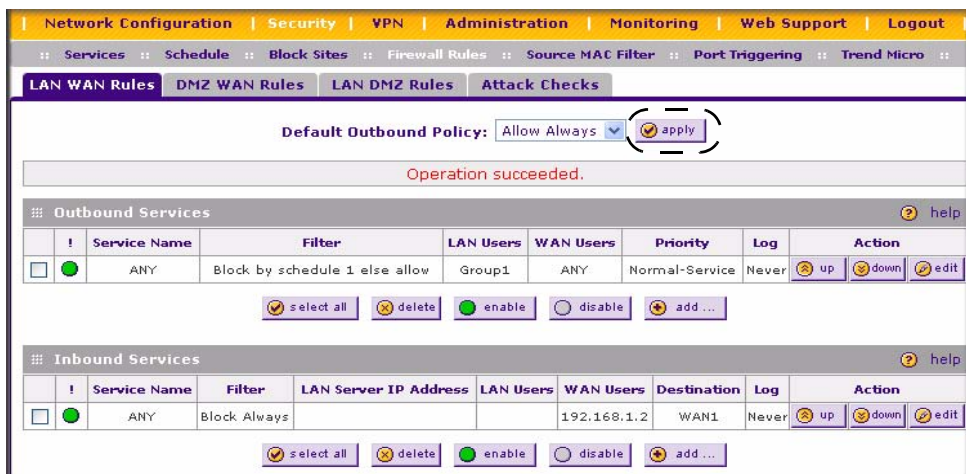


Figure 4-2

To make changes to an existing outbound or inbound service rule:

- In the **Action** column adjacent to the rule click:
 - Edit** – to make any changes to the rule definition of an existing rule. The Outbound Service screen will display containing the data for the selected rule (see [Figure 4-3 on page 4-9](#)).
 - Up** – to move the rule up one position in the table rank.
 - Down** – to move the rule down one position in the table rank.
- Check the radio box adjacent to the rule and click:
 - Click **Disable** to disable the rule. The “!” Status icon will change from green to grey, indicating that the rule is disabled. (By default, when a rule is added to the table it is automatically enabled.)
 - Click **Delete** to delete the rule.
- Click **Select All** to select all rules. A check will appear in the radio box for each rule.

LAN WAN Outbound Services Rules

You may define rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. The outbound rule will block the selected application from any internal IP LAN address to any external WAN IP address according to the schedule created in the Schedule menu.

You can also tailor these rules to your specific needs (see “[Administrator Tips](#)” on page 4-35).



Note: This feature is for Advanced Administrators only! Incorrect configuration will cause serious problems.

To create a new outbound service rule:

1. Click **Add** under the Outbound Services Table. The **Add LAN WAN Outbound Service** screen will display.

Figure 4-3

2. Complete the Outbound Service screen, and save the data (see [Table 4-1](#) on page 4-3).
3. Click **Reset** to cancel your settings and return to the previous settings.
4. Click **Apply** to save your changes and reset the fields on this screen. The new rule will be listed on the **Outbound Services** table.

LAN WAN Inbound Services Rules

This Inbound Services Rules table lists all existing rules for inbound traffic. If you have not defined any rules, no rules will be listed. By default, all inbound traffic is blocked. Remember that allowing inbound services opens holes in your firewall. Only enable those ports that are necessary for your network.

To create a new inbound service rule:

1. Click **Add** under the Inbound Services Table. The **Add LAN WAN Inbound Service** screen will display.

The screenshot shows the 'Edit LAN WAN Inbound Service' configuration window. At the top, a red message bar says 'Operation succeeded.' Below that is a tab labeled 'Inbound Service' with a help icon. The main area contains the following settings:

- Service: ANY
- Action: BLOCK by schedule, otherwise allow
- Select Schedule: Schedule 1
- Send to LAN Server: 192.168.2.1
- Translate to Port Number:
- WAN Destination IP Address: WAN1
- LAN Users: Any
- WAN Users: Any
- Log: Never
- Start: [][][][]
- Finish: [][][][]
- Start: [][][][]
- Finish: [][][][]

At the bottom, there are two buttons: 'Apply' and 'Reset'.

Figure 4-4

2. Complete the Add WAN LAN Inbound Services screen (see [Table 4-2 on page 4-5](#)).
3. Click **Reset** to cancel your settings and return to the previous settings.
4. Click **Apply** to save your changes and reset the fields on this screen. The new rule will be listed on the **Inbound Services** table.

Setting DMZ WAN Rules

The firewall rules for traffic between the DMZ and the WAN/Internet are configured on the **DMZ WAN Rules** screen. The Default Outbound Policy is to allow all traffic from and to the Internet to pass through. Firewall rules can then be applied to block specific types of traffic from either going

out from the DMZ to the Internet (Outbound) or coming in from the Internet to the DMZ (Inbound). The default outbound policy can be changed to block all outbound traffic and enable only specific services to pass through the router by adding an Outbound services Rule.

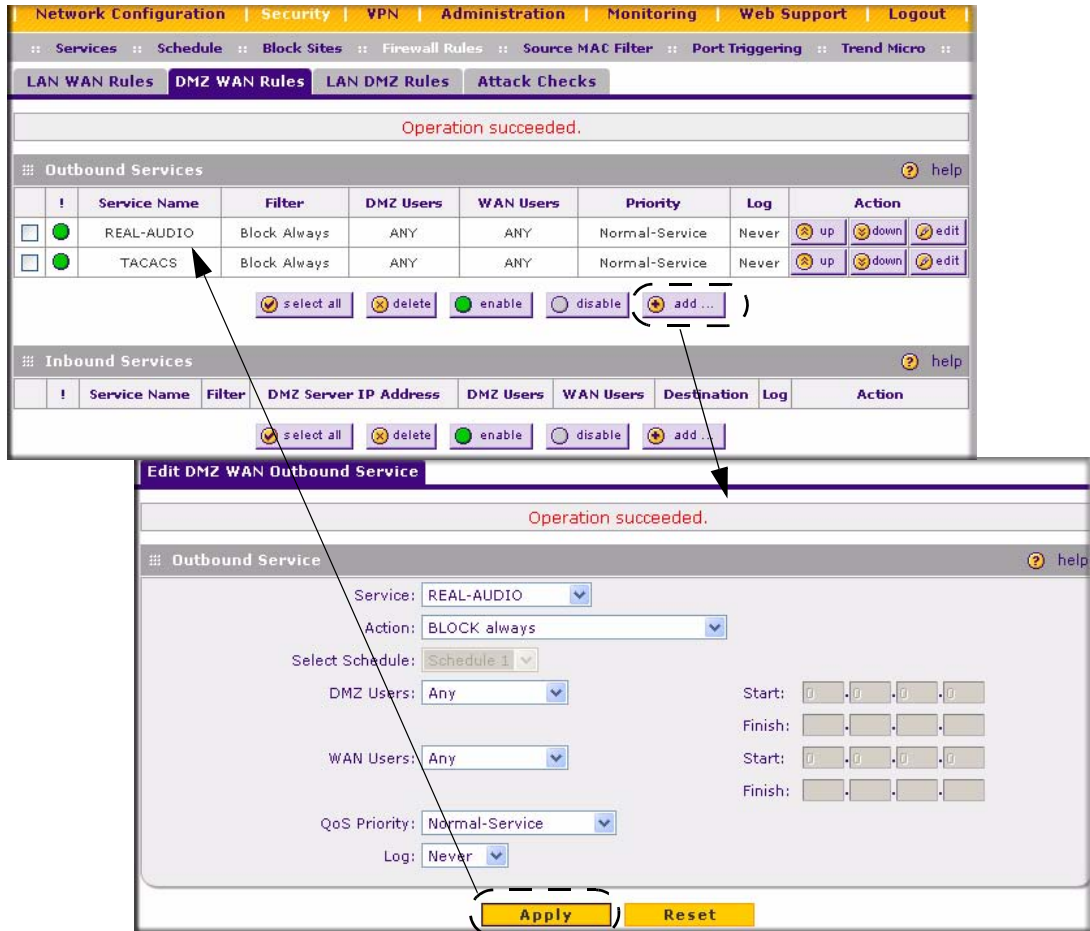


Figure 4-5

To change the Default Outbound Policy:

1. Select **Security** from the main menu, **Firewall Rules** from the submenu and then select the **DMZ WAN Rules** tab. The **DMZ WAN Rules** screen will display.
2. Click **Add** under the **Outbound Services** table. The **Add DMZ WAN Outbound Services** screen will display.
3. Accept the default settings to block all services or select a specific service to block from the Services pull-down menu.
4. Click **Apply**. The Block Always rule will appear in the Outbound Services table. The rule is automatically enabled.

The procedures described in “[Setting LAN WAN Rules](#)” on page 4-7 for setting inbound and outbound rules on the standard LAN firewall are the same as the procedures used for setting inbound and outbound rules on the DMZ port firewall.

Setting LAN DMZ Rules

The LAN DMZ Rules screen allows you to create rules that define the movement of traffic between the LAN and the DMZ. The Default Outbound and Inbound Policies is to allow all traffic between the local LAN and DMZ network. Firewall rules can then be applied to block specific types of traffic from either going out from the LAN to the DMZ (Outbound) or coming in from the DMZ to the LAN (Inbound).

To access the **LAN DMZ Rules** screen:

1. Select **Security** on the main menu, then select **Firewall Rules** and click the **LAN DMZ Rules** tab. The **LAN DMZ Rules** screen will display showing the both the Outbound Services and Inbound Services tables.

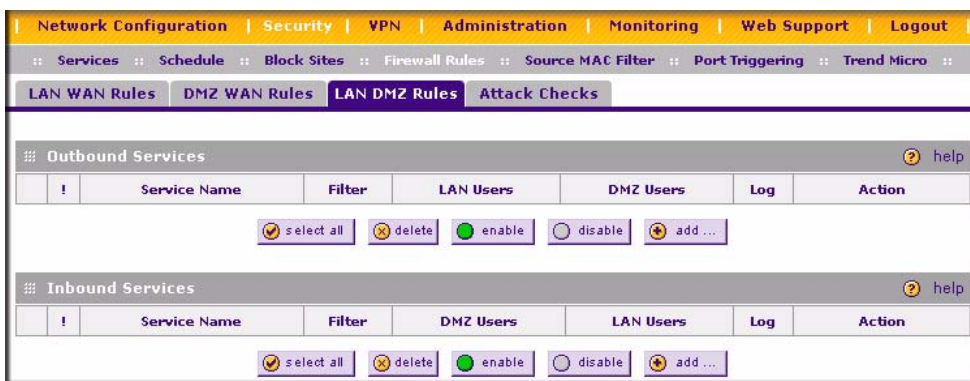


Figure 4-6

To make changes to an existing outbound or inbound LAN DMZ service rule:

1. In the **Action** column adjacent to the rule click:
 - **Edit** – to make any changes to the rule definition. The Outbound Service screen will display containing the data for the selected rule “[Outbound Rules \(Service Blocking\)](#)” on [page 4-2](#)).
 - **Up** – to move the rule up one position in the table rank.
 - **Down** – to move the rule down one position in the table rank.
2. Check the radio box adjacent to the rule and:
 - Click **Disable** to disable the rule. The “!” Status icon will change from green to grey, indicating that the rule is disabled. (By default, when a rule is added to the table it is automatically enabled.)
 - Click **Delete** to delete the rule.
3. Click **Select All** to select all rules. A check will appear in the radio box for each rule.

LAN DMZ Outbound Services Rules

To create a new outbound LAN DMZ service rule:

1. Click **Add** under the Outbound Services Table. The **Add LAN DMZ Outbound Service** screen will display.

The screenshot shows the 'Add LAN DMZ Outbound Service' configuration window. At the top, a message bar indicates 'Operation succeeded.' The main configuration area is titled 'Outbound Service' and includes the following fields:

- Service: ANY (dropdown)
- Action: BLOCK always (dropdown)
- Select Schedule: Schedule 1 (dropdown)
- LAN Users: Any (dropdown)
- DMZ Users: Any (dropdown)
- Log: Never (dropdown)
- Start and Finish time fields for both LAN and DMZ users, each with four input boxes.

At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

Figure 4-7

2. Complete the Outbound Service screen, and save the data (see [“Outbound Rules \(Service Blocking\)”](#) on page 4-2).
3. Click **Reset** to cancel your settings and return to the previous settings.
4. Click **Apply** to save your changes and reset the fields on this screen. The new rule will be listed on the **Outbound Services** table.

LAN DMZ Inbound Services Rules

To define an Inbound LAN DMZ Rule:

1. Click **Add** under the **Inbound Services** table. The **Add LAN DMZ Inbound Service** screen will display.
2. Complete the Inbound Service screen and save the data (see [“Inbound Rules \(Port Forwarding\)”](#) on page 4-4).
3. Click **Reset** to cancel your settings and return to the previous settings.
4. Click **Apply** to save your settings. The new rule will be added to the **Inbound Services table**.

Attack Checks

This screen allows you to specify whether or not the router should be protected against common attacks in the DMZ, LAN and WAN networks. The various types of attack checks are listed on the **Attack Checks** screen and defined below:

- **WAN Security Checks**
 - **Respond To Ping On Internet Ports.** If you want the router to respond to a “Ping” from the Internet, click this check box. This can be used as a diagnostic tool. You shouldn't check this box unless you have a specific reason to do so.
 - **Enable Stealth Mode.** If enabled, the router will not respond to port scans from the WAN, thus making it less susceptible to discovery and attacks.
 - **Block TCP Flood.** A SYN flood is a form of denial of service attack in which an attacker sends a succession of SYN requests to a target system. When the system responds, the attacker doesn't complete the connections, thus leaving the connection half-open and flooding the server with SYN messages. No legitimate connections can then be made.

When enabled, the router will drop all invalid TCP packets and will be protected from a SYN flood attack.

- **LAN Security Checks.** A UDP flood is a form of denial of service attack that can be initiated when one machine sends a large number of UDP packets to random ports on a remote host. As a result, the distant host will (1) check for the application listening at that port, (2) see that no application is listening at that port and (3) reply with an ICMP Destination Unreachable packet.

When the victimized system is flooded, it is forced to send many ICMP packets, eventually making it unreachable by other clients. The attacker may also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return packets do not reach him, thus making the attacker's network location anonymous.

If enabled, the router will not accept more than 20 simultaneous, active UDP connections from a single computer on the LAN.

- **VPN Pass through.** When the router is in NAT mode, all packets going to the Remote VPN Gateway are first filtered through NAT and then encrypted per the VPN policy.

For example, if a VPN Client or Gateway on the LAN side of this router wants to connect to another VPN endpoint on the WAN (placing this router between two VPN end points), encrypted packets are sent to this router. Since this router filters the encrypted packets through NAT, the packets become invalid unless VPN Pass through is enabled.

When enabled, the VPN tunnel will pass the VPN traffic without any filtering. Tunnels can be:

- IPSec
- PPTP
- L2TP

To enable the appropriate Attack Checks for your environment:

1. Select **Security** from the main menu, **Firewall Rules** from the submenu and then the **Attack Checks** tab. The **Attack Checks** screen will display.
2. Check the radio boxes of the Attack Checks you wish to initiate.

3. Click **Apply** to save your settings.



Figure 4-8

Inbound Rules Examples

LAN WAN Inbound Rule: Hosting A Local Public Web Server

If you host a public Web server on your local network, you can define a rule to allow inbound Web (HTTP) requests from any outside IP address to the IP address of your Web server at any time of day. This rule is shown in [Figure 4-9](#).

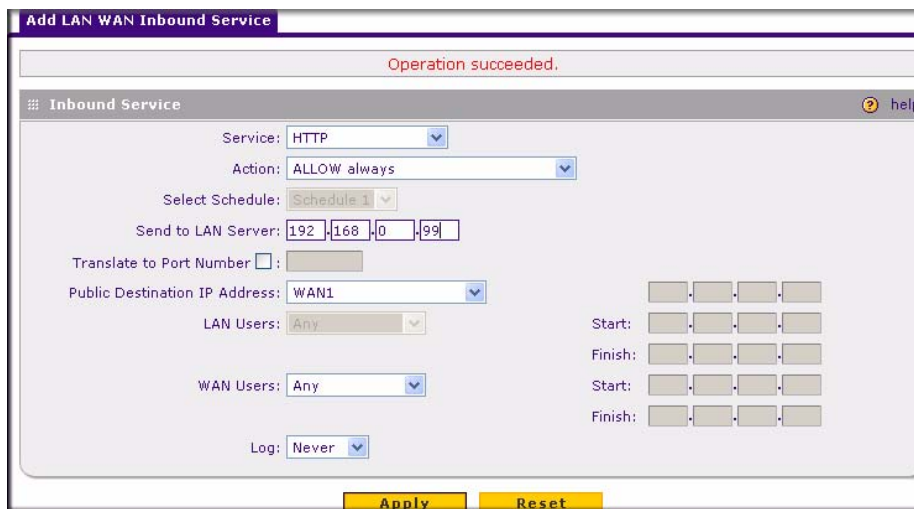


Figure 4-9

LAN WAN Inbound Rule: Allowing Videoconference from Restricted Addresses

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule. In the example, CU-SeeMe connections are allowed only from a specified range of external IP addresses.

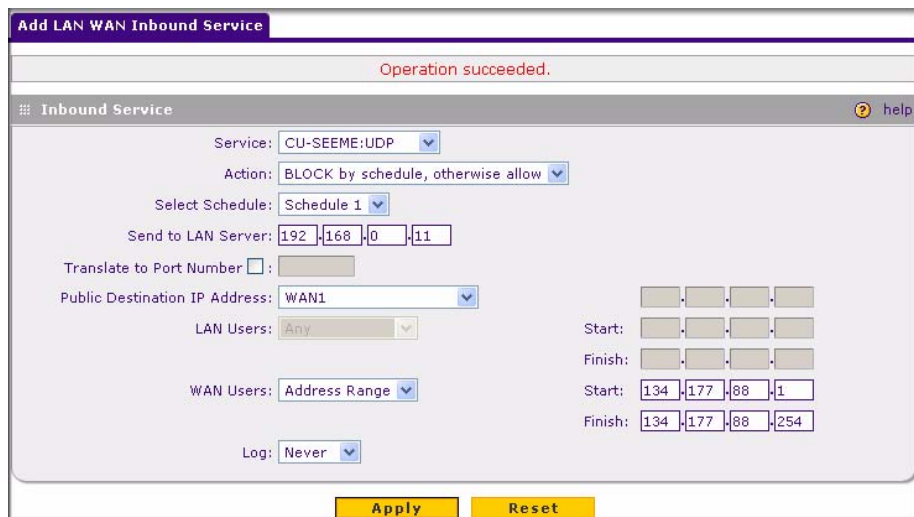


Figure 4-10

LAN WAN or DMZ WAN Inbound Rule: Setting Up One-to-One NAT Mapping


In this example, we will configure multi-NAT to support multiple public IP addresses on one WAN interface. By creating an inbound rule, we will configure the firewall to host an additional public IP address and associate this address with a Web server on the LAN.

If you arrange with your ISP to have more than one public IP address for your use, you can use the additional public IP addresses to map to servers on your LAN or DMZ. One of these public IP addresses will be used as the primary IP address of the router. This address will be used to provide Internet access to your LAN PCs through NAT. The other addresses are available to map to your servers.

The following addressing scheme is used to illustrate this procedure:

- Netgear FVX538 ProSafe VPN Firewall
 - WAN1 IP address: 10.1.0.118
 - LAN IP address subnet: 192.168.1.1; subnet 255.255.255.0
 - DMZ IP address subnet: 192.168.10.1; subnet 255.255.255.0

- Web server PC on the firewall's LAN
 - LAN IP address: 192.168.1.2
 - DMZ IP Address: 192.168.10.2
 - Access to Web server is (simulated) public IP address: 10.1.0.52



Tip: If you arrange with your ISP to have more than one public IP address for your use, you can use the additional public IP addresses to map to servers on your LAN or DMZ. One of these public IP addresses will be used as the primary IP address of the router which will be used to provide Internet access to your LAN PCs through NAT. The other addresses are available to map to your servers.

To configure the FVX538 for additional IP addresses:

1. Select **Security** from the main menu and **Firewall Rules** from the submenu.
2. If your server is to be on your LAN, select **LAN WAN Rules**.
If your server is to be on your DMZ, select **DMZ WAN Rules**.
3. Click **Add** under the **Inbound Services** table. The **Add LAN WAN Inbound Service** screen will display.
4. From the Service pull-down menu, select the HTTP service for a Web server.

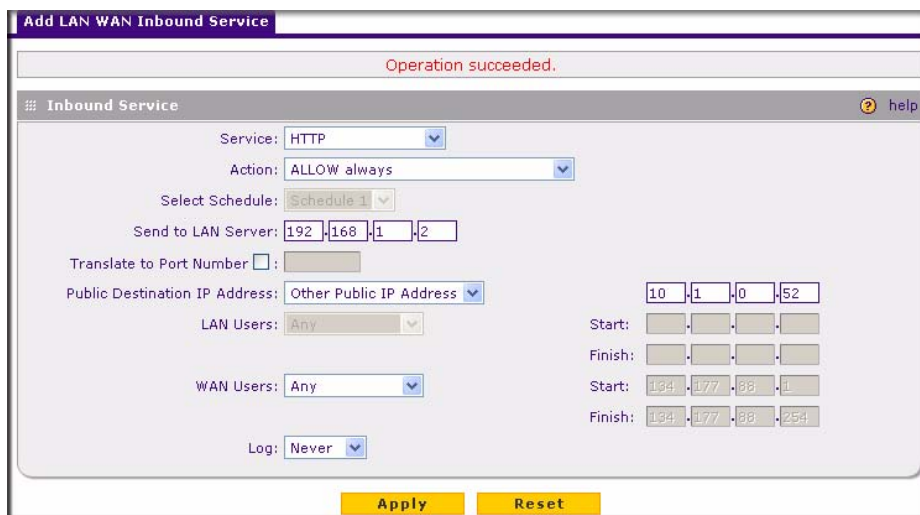


Figure 4-11

5. From the Action pull-down menu, select Allow Always.

6. In the Send to LAN Server field, enter the local IP address of your Web server PC.
7. From the Public Destination IP Address pull down menu, choose Other Public IP Address.
8. Enter one of your public Internet addresses that will be used by clients on the Internet to reach your Web server.
9. Click **Apply**.

Your rule will now appear in the Inbound Services table of the Rules menu (see [Figure 4-12](#)). This rule is different from a normal inbound port forwarding rule in that the Destination box contains an IP Address other than your normal WAN IP Address.

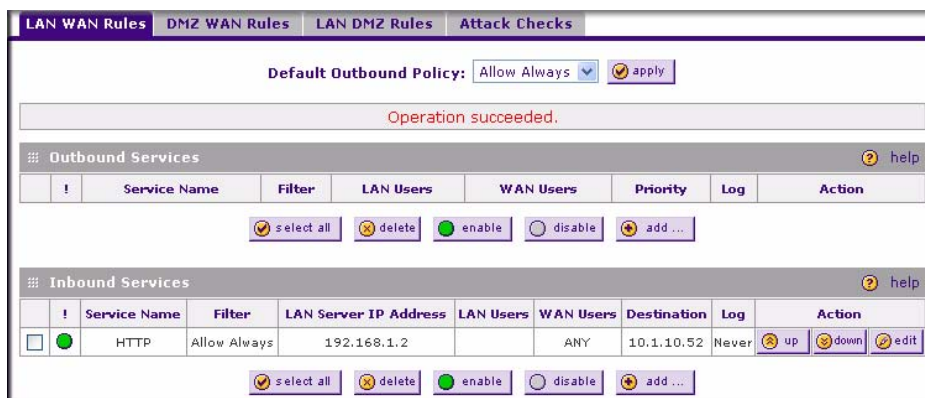


Figure 4-12

To test the connection from a PC on the Internet, type **http://<IP_address>**, where **<IP_address>** is the public IP address you have mapped to your Web server. You should see the home page of your Web server.

LAN WAN or DMZ WAN Inbound Rule: Specifying an Exposed Host

Specifying an exposed host allows you to set up a computer or server that is available to anyone on the Internet for services that you have not yet defined.

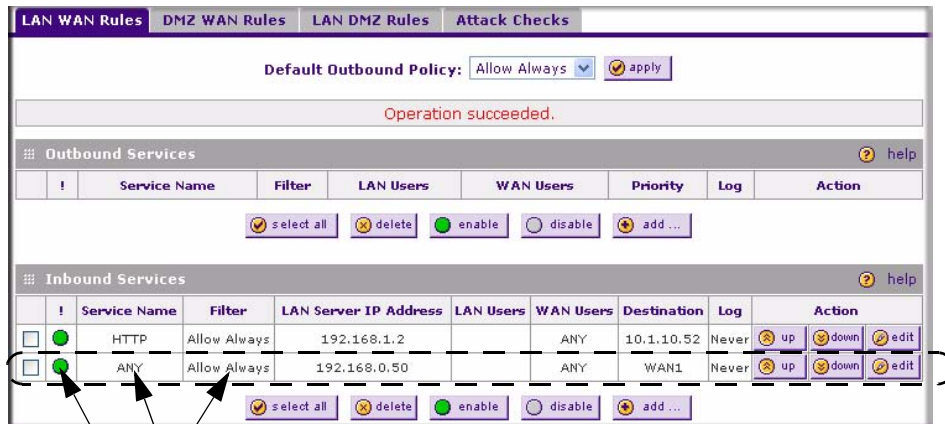
To expose one of the PCs on your LAN or DMZ as this host:

1. Create an inbound rule that allows all protocols.

- Place the rule below all other inbound rules.

➔

Note: For security, NETGEAR strongly recommends that you avoid creating an exposed host. When a computer is designated as the exposed host, it loses much of the protection of the firewall and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.



- Select Any and Allow Always (or Allow by Schedule)
- Place rule below all other inbound rules

Figure 4-13

Outbound Rules Example

Outbound rules let you prevent users from using applications such as Instant Messenger, Real Audio or other non-essential sites.

LAN WAN Outbound Rule: Blocking Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you have created in the Schedule menu. You can also have the firewall log any attempt to use Instant Messenger during that blocked period.

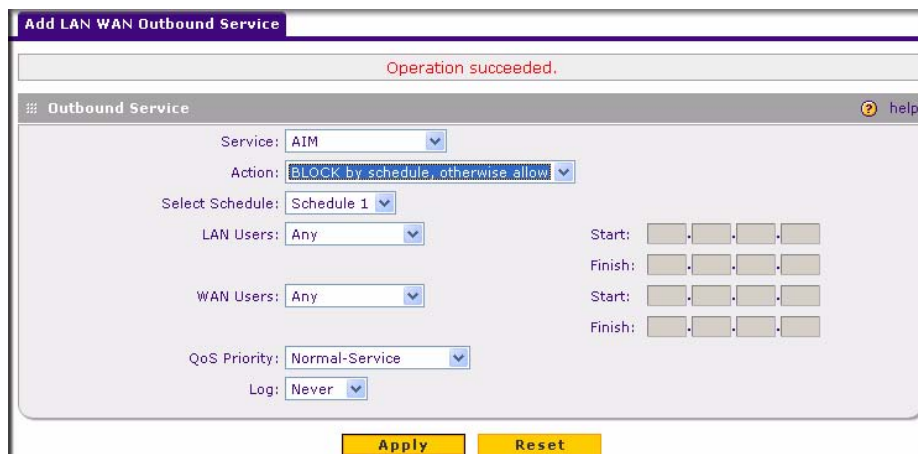


Figure 4-14

Adding Customized Services

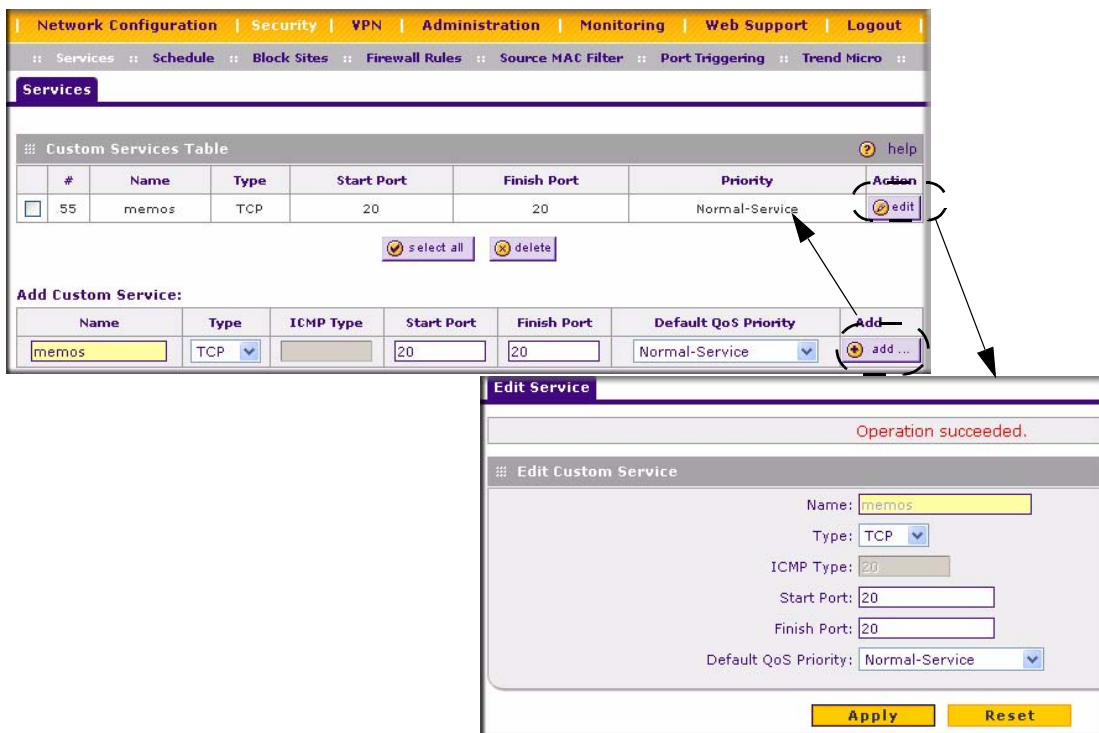
Services are functions performed by server computers at the request of client computers. You can configure up to 125 custom services.

For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the FVX538 already holds a list of many service port numbers, you are not limited to these choices. Use the Services screen to add additional services and applications to the list for use in defining firewall rules. The Services menu shows a list of services that you have defined, as shown in [Figure 4-15](#).

To define a new service, first you must determine which port number or range of numbers is used by the application. This information can usually be determined by contacting the publisher of the application or from user groups of newsgroups. When you have the port number information, you can enter it on the **Services** screen.

**Figure 4-15**

To add a customized service:

1. Select **Security** from the main menu and **Services** from the submenu. The **Services** screen will display.
2. In the **Add Custom Service** table, enter a descriptive name for the service (this is for your convenience).
3. Select the Layer 3 Protocol that the service uses as its transport protocol. It can be TCP, UDP or ICMP.
4. Enter the first TCP or UDP port of the range that the service uses. If the service uses only one port, then the Start Port and the Finish Port will be the same.
5. Enter the last port of the range that the service uses. If the service only uses a single port number, enter the same number in both fields.
6. Click **Add**. The new custom service will be added to the Custom Services Table.

To edit the parameters of a service:

1. In the Custom Services Table, click the **Edit** icon adjacent to the service you want to edit. The **Edit Service** screen will display.
2. Modify the parameters you wish to change.
3. Click **Reset** to cancel the changes and restore the previous settings.
4. Click **Apply** to confirm your changes. The modified service will display in the Custom Services Table.

Setting Quality of Service (QoS) Priorities

The Quality of Service (QoS) Priorities setting determines the priority of a service, which in turn, determines the quality of that service for the traffic passing through the firewall. The user can change this priority

- On the **Services** screen in the Custom Services Table for customized services (see [Figure 4-15](#)).
- On the **Add LAN WAN Outbound Services** screen (see [Figure 4-3](#).)
- On the **Add DMZ WAN Outbound Services** screen (see [Figure 4-5](#))

The QoS priority definition for a service determines the queue that is used for the traffic passing through the VPN firewall. A priority is assigned to IP packets using this service. Priorities are defined by the “Type of Service (ToS) in the Internet Protocol Suite” standards, RFC 1349. A ToS priority for traffic passing through the VPN firewall is one of the following:

- **Normal-Service:** No special priority given to the traffic. The IP packets for services with this priority are marked with a ToS value of 0.
- **Minimize-Cost:** Used when data has to be transferred over a link that has a lower “cost”. The IP packets for services with this priority are marked with a ToS value of 1.
- **Maximize-Reliability:** Used when data needs to travel to the destination over a reliable link and with little or no retransmission. The IP packets for services with this priority are marked with a ToS value of 2.
- **Maximize-Throughput:** Used when the volume of data transferred during an interval is important even if the latency over the link is high. The IP packets for services with this priority are marked with a ToS value of 4.
- **Minimize-Delay:** Used when the time required (latency) for the packet to reach the destination must be low. The IP packets for services with this priority are marked with a ToS value of 8.

Setting a Schedule to Block or Allow Specific Traffic

If you enabled Content Filtering in the Block Sites menu, or if you defined an outbound or inbound rule to use a schedule, you can set up a schedule for when blocking occurs or when access is restricted. The firewall allows you to specify when blocking will be enforced by configuring one of the Schedules—Schedule 1, Schedule 2 or Schedule 3.

To invoke rules and block keywords or Internet domains based on a schedule:

1. Select **Security** from the main menu and **Schedule** from the sub-menu. The **Schedule 1** screen will display.
2. Check the radio button for All Days or Specific Days. If you chose Specific Days, check the radio button for each day you want the schedule to be in effect.
3. Check the radio button to schedule the time of day: All Day, or Specific Times. If you chose Specific Times, enter the Start Time and End Time fields (Hour, Minute, AM/PM), which will limit access during certain times for the selected days.
4. Click **Reset** to cancel your settings and revert to the previous settings.
5. Click **Apply** to save your settings to **Schedule 1**.

Repeat these 5 steps to set to a schedule for **Schedule 2** and **Schedule 3**.

The screenshot shows the 'Schedule 1' configuration page. The 'Scheduled Days' section is active, with 'All Days' selected. The 'Scheduled Time of Day' section is also active, with 'Specific Times' selected. The Start Time is set to 12:00 AM and the End Time is set to 12:00 PM. The 'Apply' and 'Reset' buttons are visible at the bottom.

Figure 4-16

Setting Block Sites (Content Filtering)

If you want to restrict internal LAN users from access to certain sites on the Internet, you can use the VPN firewall's Content Filtering and Web Components filtering. By default, these features are disabled; all requested traffic from any Web site is allowed. If you enable one or more of these features and users try to access a blocked site, they will see a "Blocked by NETGEAR" message.

Several types of blocking are available:

- **Web Components** blocking. You can block the following Web component types: Proxy, Java, ActiveX, and Cookies. Even sites on the Trusted Domains list will be subject to Web Components blocking when the blocking of a particular Web component is enabled.
- **Keyword Blocking** (Domain Name Blocking). You can specify up to 32 words that, should they appear in the Web site name (URL) or in a newsgroup name, will cause that site or newsgroup to be blocked by the VPN firewall.

You can apply the keywords to one or more groups. Requests from the PCs in the groups for which keyword blocking has been enabled will be blocked. Blocking does not occur for the PCs that are in the groups for which keyword blocking has not been enabled.

You can bypass Keyword blocking for trusted domains by adding the exact matching domain to the list of Trusted Domains. Access to the domains or keywords on this list by PCs, even those in the groups for which keyword blocking has been enabled, will still be allowed without any blocking.

Keyword application examples:

- If the keyword "XXX" is specified, the URL <http://www.badstuff.com/xxx.html> is blocked, as is the newsgroup alt.pictures.XXX.
- If the keyword ".com" is specified, only Web sites with other domain suffixes (such as .edu or .gov) can be viewed.
- If you wish to block all Internet browsing access, enter the keyword ".".

To enable Content Filtering:

1. Select **Security** from the main menu and **Block Sites** from the sub-menu. The **Block Sites** screen will display.
2. Check the **Yes** radio button to enable Content Filtering.
3. Check the radio boxes of any Web Components you wish to block.
4. Check the radio buttons of the groups to which you wish to apply Keyword Blocking. Click **Enable** to activate Keyword blocking (or disable to deactivate Keyword Blocking).

5. Build your list of blocked Keywords or Domain Names in the **Blocked Keyword** fields. After each entry, click **Add**. The Keyword or Domain name will be added to the **Blocked Keywords** table. (You can also edit an entry by clicking **Edit** in the Action column adjacent to the entry.)
6. Build a list of Trusted Domains in the **Trusted Domains** fields. After each entry, click **Add**. The Trusted Domain will appear in the **Trusted Domains** table. (You can also edit any entry by clicking **Edit** in the Action column adjacent to the entry.)
7. Click **Reset** to cancel your changes and revert to the previous settings.
8. Click **Apply** to save your settings.

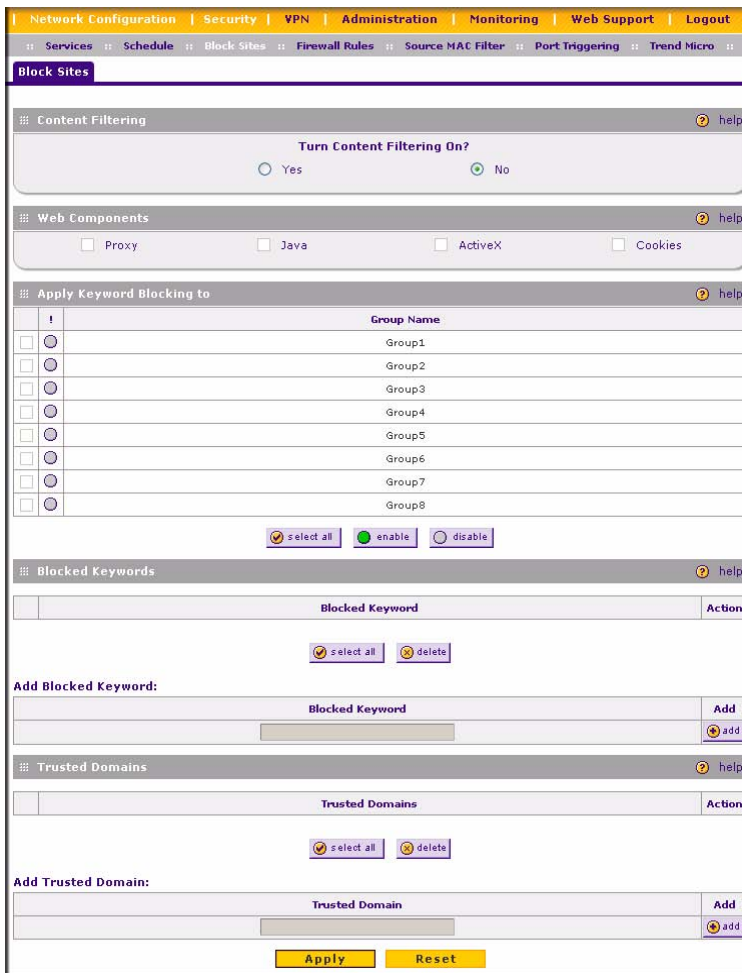


Figure 4-17

Enabling Source MAC Filtering

Source MAC Filter allows you to filter out traffic coming from certain known machines or devices.

- By default, the source MAC address filter is disabled. All the traffic received from PCs with any MAC address is allowed.
- When enabled, traffic will be dropped coming from any computers or devices whose MAC addresses are listed in **Available MAC Addresses to be Blocked** table.

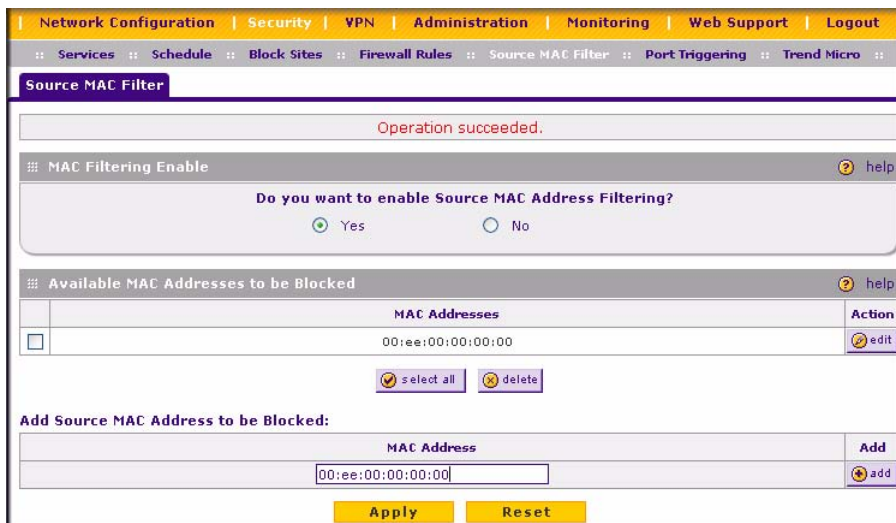



Figure 4-18

	<p>Note: For additional ways of restricting outbound traffic, see “Outbound Rules (Service Blocking)” on page 4-2</p>
---	--

To enable MAC filtering and add MAC addresses to be blocked:

1. Select **Security** from the main menu and **Source MAC Filter** from the sub-menu. The **Source MAC Filter** screen will display.
2. Check the Yes radio box in the **MAC Filtering Enable** section.

3. Build your list of Source MAC Addresses to be block by entering the first MAC address in the **MAC Address** field in the form xx:xx:xx:xx:xx:xx where x is a numeric (0 to 9) or an alphabet between and a and f (inclusive), for example: 00:e0:4c:69:0a:
4. Click **Add**. The Mac Address will be added to the **Available MAC Addresses to be Blocked** table. (You can edit the MAC address by clicking **Edit** in the Action column adjacent to the MAC Address.)
5. Click **Reset** to cancel a MAC address entry before adding it to the table.
6. Click **Apply** to save your settings.

To remove an entry from the table, select the MAC address entry and click **Delete**.

To select all the list of MAC addresses, click **Select All**. A checkmark will appear in the box to the left of each MAC address in the **Available MAC Addresses to be Blocked** table.

Port Triggering

Port triggering allows some applications running on a LAN network to be available to external applications that would otherwise be partially blocked by the firewall. Using this feature requires that you know the port numbers used by the Application.

Once configured, Port Triggering operates as follows:

1. A PC makes an outgoing connection using a port number defined in the Port Triggering table.
2. The VPN firewall records this connection, opens the additional INCOMING port or ports associated with this entry in the Port Triggering table, and associates them with the PC.
3. The remote system receives the PCs request and responds using the different port numbers that you have now opened.
4. The VPN firewall matches the response to the previous request, and forwards the response to the PC.

Without Port Triggering, this response would be treated as a new connection request rather than a response. As such, it would be handled in accordance with the Port Forwarding rules:

- Only one PC can use a Port Triggering application at any time.

- After a PC has finished using a Port Triggering application, there is a Time-out period before the application can be used by another PC. This is required because this Router cannot be sure when the application has terminated.



Note: For additional ways of allowing inbound traffic, see [“Inbound Rules \(Port Forwarding\)”](#) on page 4-4.

To add a Port Triggering Rule:

1. Select **Security** from the main menu and **Port Triggering** from the submenu. The **Port Triggering** screen will display.
1. Enter a user-defined name for this rule in the **Name** field.
2. From the **Enable** pull-down menu, indicate if the rule is enabled or disabled.

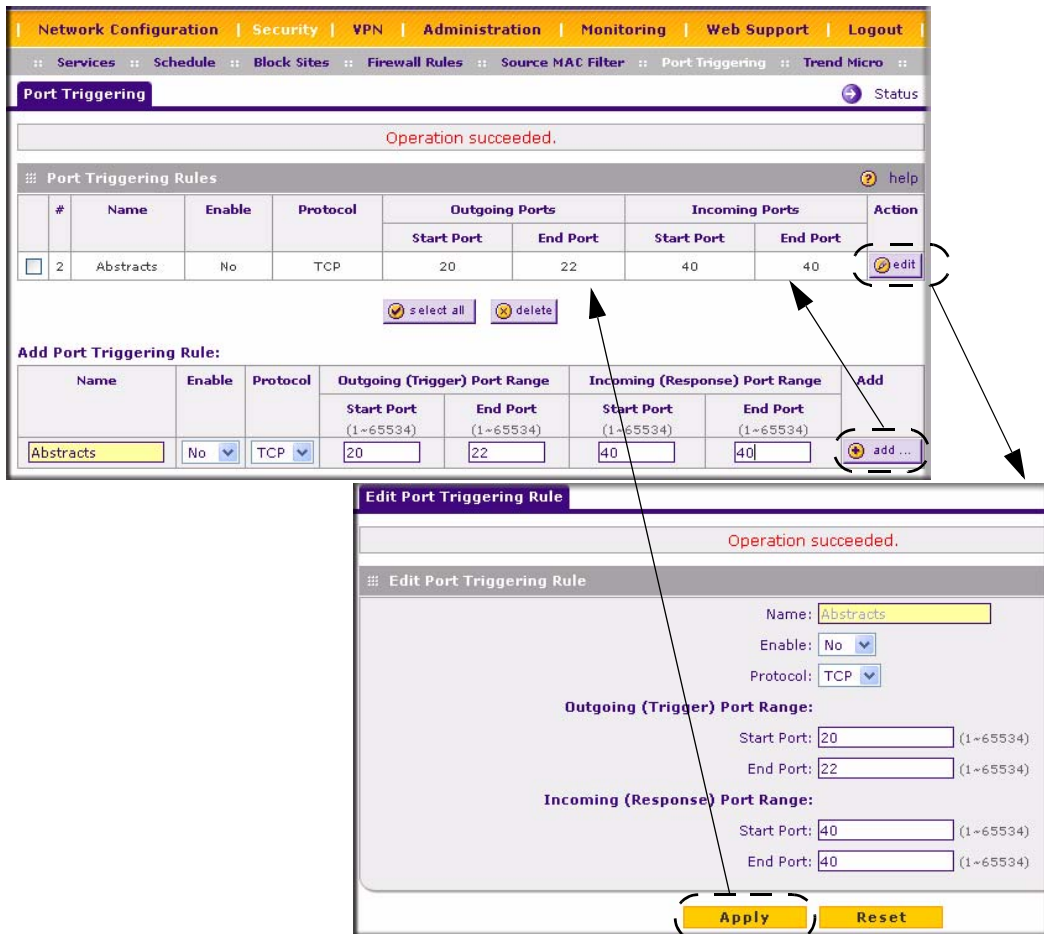


Figure 4-19

- From the **Protocol** pull-down menu, select either TCP or UDP protocol.
- In the **Outgoing (Trigger) Port Range** fields:
 - Enter the **Start Port** range (1 - 65534).
 - Enter the **End Port** range (1 - 65534).
- In the **Incoming (Response) Port Range** fields:
 - Enter the **Start Port** range (1 - 65534).
 - Enter the **End Port** range (1 - 65534).

6. Click **Add**. The Port Triggering Rule will be added to the **Port Triggering Rules** table.

To edit or modify a rule:

1. Click **Edit** in the Action column opposite the rule you wish to edit. The **Edit Port Triggering Rule** screen will display.
2. Modify any of the fields for this rule.
3. Click **Reset** to cancel any changes and return to the previous settings.
4. Click **Apply** to save your modifications. Your changes will appear in the **Port Triggering Rules** table.

To check the status of the Port Triggering rules, click the **Status** link on the **Port Triggering** screen.

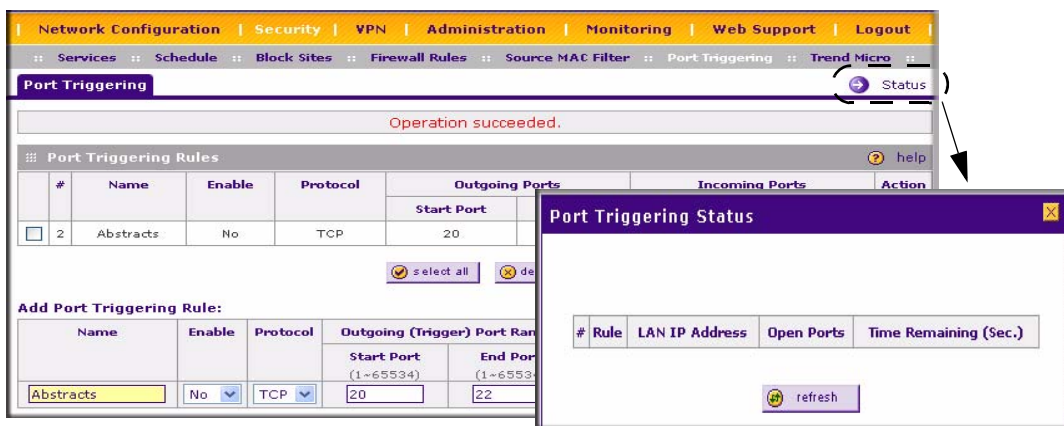


Figure 4-20

E-Mail Notifications of Event Logs and Alerts

The Firewall Logs can be configured to log and then e-mail denial of access, general attack information, and other information to a specified e-mail address. For example, your VPN firewall will log security-related events such as: accepted and dropped packets on different segments of your LAN or DMZ; denied incoming and outgoing service requests; hacker probes and Login attempts; and other general information based on the settings you input on the **Firewall Logs & E-mail** screen. In addition, if you have set up Content Filtering on the Block Sites screen (see [“Setting Block Sites \(Content Filtering\)”](#) on page 4-25), a log will be generated when someone on your network tries to access a blocked site.

You must have e-mail notification enabled to receive the logs in an e-mail message. If you don't have e-mail notification enabled, you can view the logs on the **Logs** screen (see [Figure 4-22 on page 4-34](#)). Selecting all events will increase the size of the log, so it is good practice to select only those events which are required.

The screenshot shows the 'Firewall Logs & E-mail' configuration page. At the top, there is a navigation bar with tabs for Network Configuration, Security, VPN, Administration, Monitoring, Web Support, and Logout. Below this is a breadcrumb trail: Router Status > Traffic Meter > Diagnostics > Firewall Logs & E-mail > VPN Logs. The main content area is titled 'Firewall Logs & E-mail' and includes a 'View Log' button. The configuration is organized into several sections:

- Log Options:** A text field for 'Log Identifier' containing 'FVX538'.
- Send logs according to this schedule:** A dropdown for 'Unit' set to 'Never', a dropdown for 'Day' set to 'Sunday', and a 'Time' dropdown set to '1:00' with radio buttons for 'a.m.' and 'p.m.'.
- Security Logs:** Two columns of checkboxes for 'Accepted Packets' and 'Dropped Packets', each with options for LAN to WAN, LAN to DMZ, DMZ to WAN, WAN to LAN, DMZ to LAN, and WAN to DMZ.
- System Logs:** A list of checkboxes for events such as 'Change of time by NTP', 'Login attempts', 'Secure Login attempts', 'Reboots', 'Inbound WAN Packets Dropped', and 'Inbound LAN Packets Dropped'.
- Enable E-Mail Logs:** A section with a radio button for 'Do you want logs to be emailed to you?' set to 'Yes'. It includes fields for 'E-Mail Server Address', 'Return E-Mail Address', and 'Send to E-Mail Address'. There are radio buttons for 'No Authentication', 'Login Plain', and 'CRAM-MD5', along with 'User Name' and 'Password' fields. A checkbox for 'Respond to Identd from SMTP Server' is also present.
- Enable SysLogs:** A section with a radio button for 'Do you want to enable syslog?' set to 'Yes'. It includes fields for 'SysLog Server' and a dropdown for 'SysLog Facility' set to 'Local0'.

At the bottom of the page are two buttons: 'Apply' and 'Reset'.

Figure 4-21

To set up Firewall Logs and E-mail alerts:

1. Select **Monitoring** from the main menu and then **Firewall Logs & E-mail** from the submenu. The **Firewall Logs & E-mail** screen will display.
2. Enter the name of the log in the **Log Identifier** field. Log Identifier is a mandatory field used to identify the log messages. The ID appended to log messages.

3. Enter a **Schedule** for sending the logs. From the **Unit** pull-down menu, select: Never, Hourly, Daily, or Weekly. Then fill in the Day and Time fields that correspond to your selection.
4. In the **Security Logs** section, check the network segments radio box for which you would like logs to be sent (for example, LAN to WAN under Dropped Packets).
5. In the **System Logs** section, check the radio box for the type of system events to be logged.
6. Check the **Yes** radio box to enable E-mail Logs. Then enter:
 - a. **E-mail Server address** – Enter the outgoing E-mail SMTP mail server address of your ISP (for example, 172.16.1.10). If you leave this box blank, no logs will be sent to you.
 - b. **Return E-mail Address** – Enter the e-mail address of the user.
 - c. **Send To E-mail Address** – Enter the e-mail address where the logs and alerts should be sent. You must use the full e-mail address (for example, ChrisXY@myISP.com).
7. The **No Authentication** radio box is checked by default. If your SMTP server authenticates users, uncheck the radio box by selecting the authentication type—either **Login Plain** or **CRAM-MD5**—based on your SMTP server requirements. Then enter the user name and password to be used for authentication.
8. If you want to respond to IDENT protocol, check the **Respond to Identd from SMTP Server** radio box. The Ident Protocol is an Internet protocol that helps identify the user of a particular TCP connection (a common daemon program for providing the ident service is identd).
9. You can configure the firewall to send system logs to an external PC that is running a syslog logging program. Click the **Yes** radio box to enable SysLogs and send messages to the syslog server, then:
 - a. Enter your **SysLog Server IP** address
 - b. Select the appropriate syslog facility from the **SysLog Facility** pull-down menu. The SysLog Facility levels of severity are described in [Table 4-3](#) below.
10. Click **Reset** to cancel your changes and return to the previous settings.
11. Click **Apply** to save your settings.

Table 4-3. SysLog Facility Message Levels

Numerical Code	Severity
0	Emergency: System is unusable
1	Alert: Action must be taken immediately
2	Critical: Critical conditions
3	Error: Error conditions

Table 4-3. SysLog Facility Message Levels (continued)

Numerical Code	Severity
4	Warning: Warning conditions
5	Notice: Normal but significant conditions
6	Informational: Informational messages
7	Debug: Debug level messages

To view the Firewall logs:

1. Click on the **View Log** icon opposite the **Firewall Logs & E-mail** tab. The **Logs** screen will display.
2. If the E-mail Logs options as been enabled, you can send a copy of the log by clicking **send log**.
3. Click **refresh log** to retrieve the latest update; and click **clear log** to delete all entries.

Log entries are described in [Table 4-4](#).

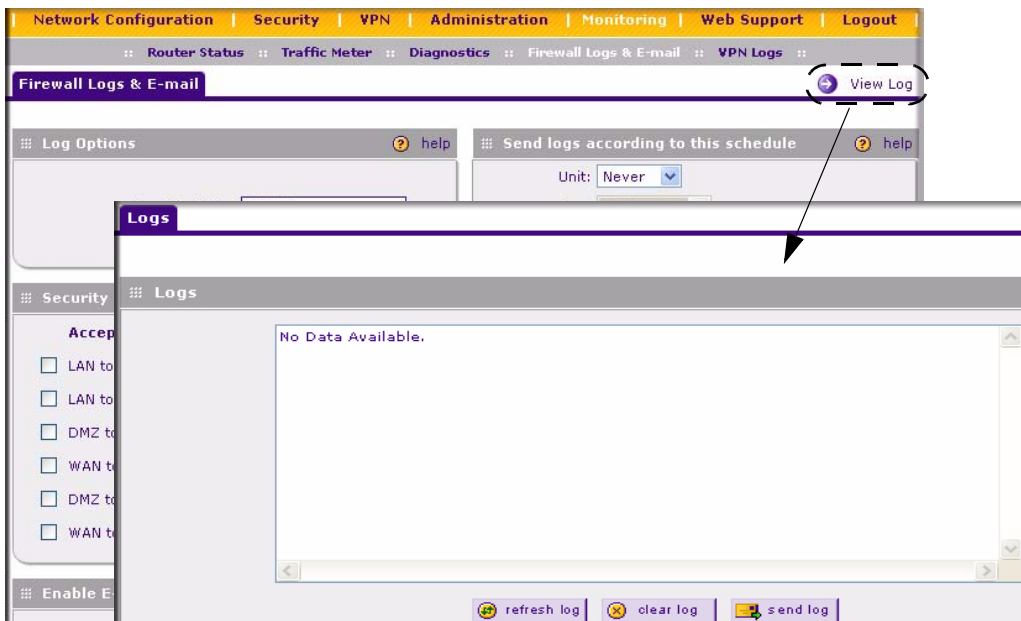
**Figure 4-22**

Table 4-4. Firewall Log Field Descriptions

Field	Description
Date and Time	The date and time the log entry was recorded.
Description or Action	The type of event and what action was taken if any.
Source IP	The IP address of the initiating device for this log entry.
Source port and interface	The service port number of the initiating device, and whether it originated from the LAN, WAN or DMZ.
Destination	The name or IP address of the destination device or Web site.
Destination port and interface	The service port number of the destination device, and whether it's on the LAN, WAN or DMZ.

Administrator Tips

Consider the following operational items:

1. As an option, you can enable remote management if you have to manage distant sites from a central location (see [“Enabling Remote Management Access”](#) on page 6-10).
2. Although rules (see [“Using Rules to Block or Allow Specific Kinds of Traffic”](#) on page 4-1) is the basic way of managing the traffic through your system, you can further refine your control with the following optional features of the VPN firewall:
 - Groups and hosts (see [“Managing Groups and Hosts \(LAN Groups\)”](#) on page 3-6)
 - Services (see [“Services-Based Rules”](#) on page 4-2)
 - Schedules (see [“Setting a Schedule to Block or Allow Specific Traffic”](#) on page 4-24)
 - Block sites (see [“Setting Block Sites \(Content Filtering\)”](#) on page 4-25)
 - Source MAC filtering (see [“Enabling Source MAC Filtering”](#) on page 4-27)
 - Port triggering (see [“Port Triggering”](#) on page 4-28)

Chapter 5

Virtual Private Networking

This chapter describes how to use the virtual private networking (VPN) features of the VPN firewall. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer.



Tip: When using dual WAN port networks, use the VPN Wizard to configure the basic parameters and then edit the VPN and IKE Policy screens for the various VPN scenarios.

Dual WAN Port Systems

The dual WAN ports in the VPN firewall can be configured for either Auto-Rollover mode for increased system reliability or Load Balancing mode for optimum bandwidth efficiency. This WAN mode choice then impacts how the VPN features must be configured.

Refer to “[Virtual Private Networks \(VPNs\)](#)” on page C-10 for an overview of the IP addressing requirements for VPN in the two WAN modes. To aid in determining the addressing requirements for your VPN Tunnel in either rollover mode or load balancing mode, see [Table 5-1](#).

Table 5-1. IP Addressing for VPNs in Dual WAN Port Systems

Configuration and WAN IP address		Rollover Mode ^a	Load Balancing Mode
VPN Road Warrior (client-to-gateway)	Fixed	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required
VPN Gateway-to-Gateway	Fixed	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required
VPN Telecommuter (client-to-gateway through a NAT router)	Fixed	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required

a. All tunnels must be re-established after a rollover using the new WAN IP address.

Figure 5-1 shows the **WAN Mode** setup screen for Auto-Rollover Mode using WAN port 1. It also shows the **Protocol Bindings** screen that displays if Load Balancing is selected. (When Load Balancing is selected, no **WAN Failure Detection Method** fields are selectable.) This setup is accomplished in “Configuring the WAN Mode (Required for Dual WAN)” on page 2-10.

Rollover Mode Setup Screen

The screenshot shows the WAN Mode configuration interface. The 'Port Mode' section has 'Auto-Rollover using WAN port: WAN1' selected. A 'view protocol bindings' link is highlighted with a dashed box and an arrow pointing to the 'WAN1 Protocol Bindings' screen below. The 'WAN Failure Detection Method' section has 'DNS lookup using configured DNS Servers' selected.

The 'WAN1 Protocol Bindings' screen shows a table for protocol bindings and an 'Add Protocol Binding' section.

#	!	Service	Source Network	Destination Network	Action
<input type="checkbox"/> select all <input type="checkbox"/> delete <input checked="" type="radio"/> enable <input type="radio"/> disable					
Add Protocol Binding:					
Service		Destination Network		Source Network	Add
ANY		Any		Any	<input type="button" value="add"/>
		Start Address:		Start Address:	
		End Address:		End Address:	

Load Balancing Setup Screen

Figure 5-1

The use of fully qualified domain names is:

- Mandatory when the WAN ports are in rollover mode (Figure 5-2 on page 5-3); also required for the VPN tunnels to fail over.

- Mandatory when the WAN ports are in load balancing mode and the IP addresses are dynamic (Figure 5-3 on page 5-3)
- Optional when the WAN ports are in load balancing mode if the IP addresses are static (Figure 5-3 on page 5-3)

See “Configuring Dynamic DNS (If Needed)” on page 2-15 for how to select and configure the Dynamic DNS service.

FVX538 Functional Block Diagram – Auto-Rollover

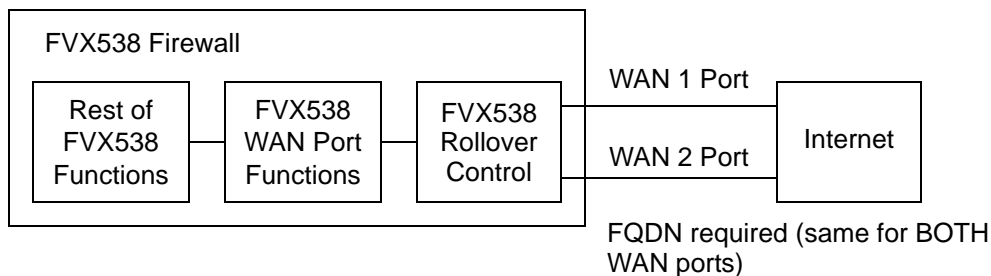


Figure 5-2

FVX538 Functional Block Diagram – Load Balancing

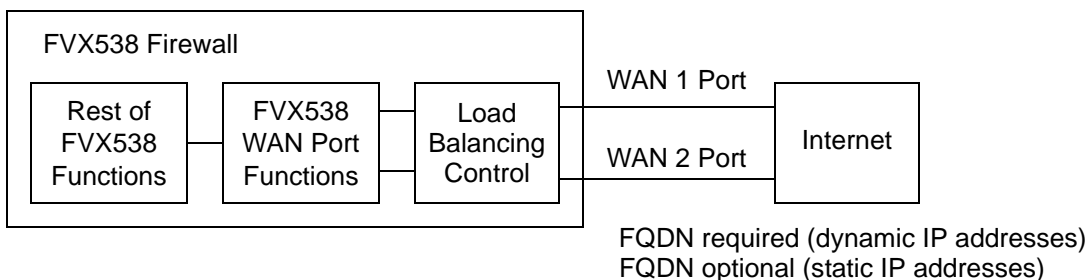


Figure 5-3

Setting up a VPN Connection using the VPN Wizard

Setting up a VPN tunnel connection requires that all settings and parameters on both sides of the VPN tunnel match or mirror each other precisely, which can be a daunting task. The VPN Wizard can assist in guiding you through the setup procedure by asking you a series of questions that will

determine the IPSec keys and VPN policies it sets up. It also will set the parameters for the network connection: Security Association, traffic selectors, authentication algorithm, and encryption. The parameters used by the VPN wizard are based on the VPNC recommendations.

Creating a VPN Tunnel to a Gateway

You can set up multiple Gateway VPN tunnel policies through the VPN Wizard. You can also set up multiple remote VPN Client policies through the VPN Wizard. A remote client policy can support up to 200 clients.

To set up a Gateway VPN Tunnel using the VPN Wizard:

1. Select **Gateway** as your **VPN tunnel connection**. The wizard needs to know if you are planning to connect to a remote Gateway or setting up the connection for a remote client/PC to establish a secure connection to this device.
2. Select a **Connection Name**. Enter an appropriate name for the connection. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the VPN settings.
3. Enter a **Pre-shared Key**. The key must be entered both here and on the remote VPN Gateway, or the remote VPN Client. This key length should be minimum 8 characters and should not exceed 49 characters. This method does not require using a CA (Certificate Authority).
4. Check the radio box for the **WAN interface** that will act as one end of this VPN tunnel: WAN 1 or WAN 2.
5. Enter the **Remote WAN IP Address or Internet Name** of the gateway you want to connect to.
 - Both the remote WAN address and your local WAN address are required. When choosing these addresses, follow the guidelines in [Table 5-1](#) above.
 - The remote WAN IP address of the Gateway must be a public address or the Internet name of the Gateway. The *Internet name* is the Fully Qualified Domain Name (FQDN) as setup in a Dynamic DNS service. Both local and remote ends should be defined as either IP addresses or Internet Names (FQDN). A combination of IP address and Internet Name is not permissible.
6. Enter the **Local WAN IP Address or Internet Name** of your gateway.

The Local WAN IP address is used in the IKE negotiation phase. Automatically, the WAN IP address assigned by your ISP may display. You can modify the address to use your FQDN; required if the WAN Mode you selected is auto-rollover.

Figure 5-4

7. Enter the **Remote LAN IP Address and Subnet Mask** of the remote gateway.

The information entered here must match the Local LAN IP and Subnet Mask of the remote gateway; otherwise the secure tunnel will fail to connect. The IP address range used on the remote LAN must be different from the IP address range used on the local LAN.

8. Click the **VPN Wizard Default Values** link at the top right of the screen to view the recommended VPNC parameters (see [Figure 5-4](#)).
9. Click **Apply** to save your settings. The **VPN Policies** screen will display showing the policy “Offsite” as enabled. Click **Edit** in the **Action** column adjacent to the policy to confirm your policy settings.

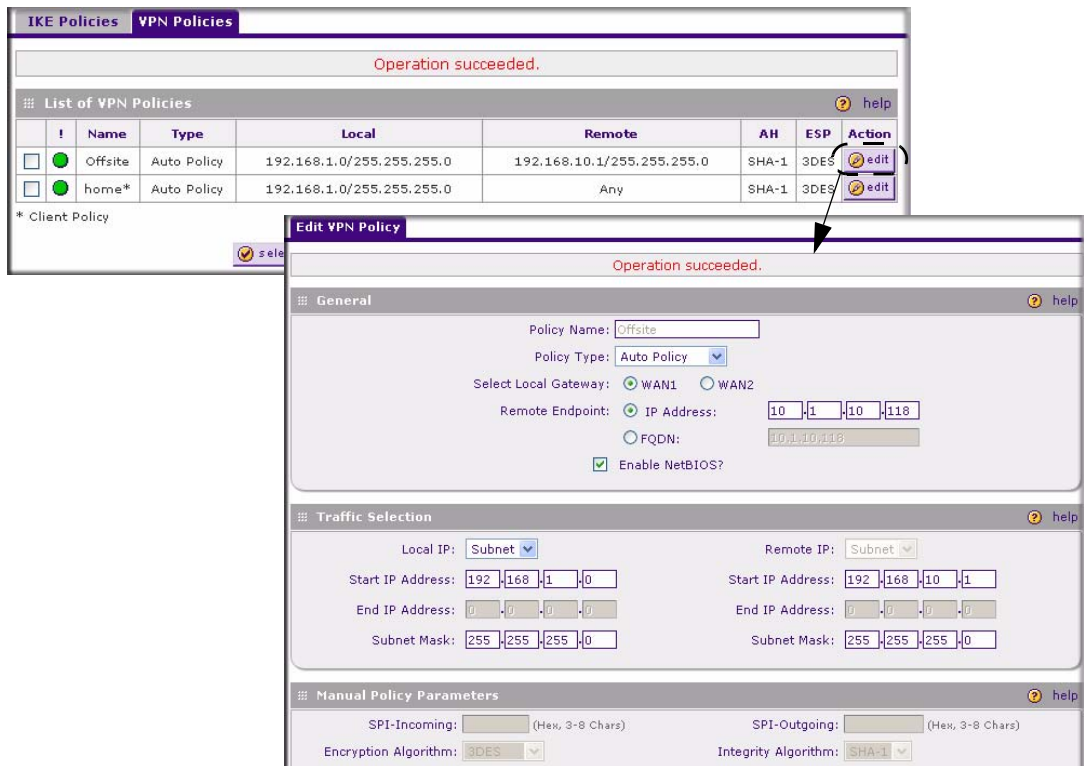


Figure 5-5

You can also view the status of your IKE Policies by clicking the **IKE Policies** tab. The **IKE Policies** screen will display. Then view or edit the parameters of the “Offsite” policy by clicking **Edit** in the **Action** column adjacent to the policy. The **Edit IKE Policy** screen will display.

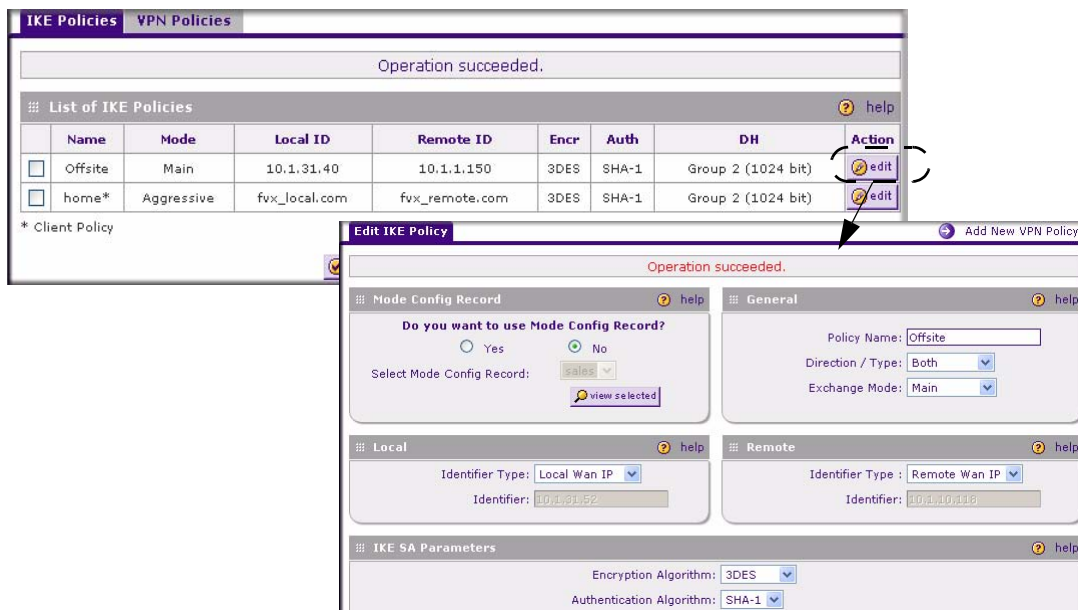


Figure 5-6

Creating a VPN Tunnel Connection to a VPN Client

You can set up multiple Gateway VPN tunnel policies through the VPN Wizard. Multiple remote VPN Client policies can also be set up through the VPN Wizard by changing the default End Point Information settings. A remote client policy can support up to 200 clients. The remote clients must configure the “Local Identity” field in their policy as “PolicyName<X>.fvx_remote.com”, where X stands for a number from 1 to 200.

As an example, if the client-type policy on the router is configured with “home” as the policy name, and if two users are required to connect using this policy, then the “Local Identity” in their policy should be configured as “home1.fvx_remote.com” and “home2.fvx_remote.com”, respectively.

To configure the VPN client:

1. Select **VPN** from the main menu and **VPN Wizard** from the submenu. The **VPN Wizard** screen will display.
2. Check the **VPN Client** radio box as your **VPN tunnel connection**. The wizard needs to know if you are planning to connect to a remote Gateway or setting up the connection for a remote client/PC to establish a secure connection to this device.

3. Select a **Connection Name**. Enter an appropriate name for the connection. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the VPN settings.

Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout

:: Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status ::

VPN Wizard VPN Wizard Default Values

About VPN Wizard help

The Wizard sets most parameters to defaults as proposed by the VPN Consortium ([VPN Consortium](#)), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the [Policies](#) menu.

This VPN tunnel will connect to the following peers:

Gateway VPN Client

Connection Name and Remote IP Type help

What is the new Connection Name?

What is the pre-shared key? (Key Length 8 - 49 Char)

This VPN tunnel will use following local WAN Interface: WAN 1 WAN 2

End Point Information help

What is the Remote Identifier Information?

What is the Local Identifier Information?

Secure Connection Remote Accessibility help

What is the remote LAN IP Address?

What is the remote LAN Subnet Mask?

Figure 5-7

4. Enter a **Pre-shared Key**. The key must be entered both here and on the remote VPN Gateway, or the remote VPN Client. This key length should be minimum 8 characters and should not exceed 49 characters. This method does not require using a CA (Certificate Authority).
5. Check the radio box of the **WAN interface** that will act as one end of this VPN tunnel: WAN 1 or WAN 2.
6. Enter the public **WAN IP** address of the gateway to which you want to connect. Alternatively, you can provide the Internet name of the gateway. The Internet name is the Fully Qualified Domain Name (FQDN); for example, vpn.netgear.com.
7. Enter the **Local WAN IP Address** or Internet name. Both local and remote ends should be defined as either IP addresses or Internet Names (FQDN). A combination of IP address and Internet Name is not permissible.

8. Click **Apply**. The **VPN Policies** screen will display showing that the Client policy “home” has been added and enabled. Click **Edit** in the **Action** column adjacent to the “home” policy to view the “home” policy parameters. It should not be necessary to make any changes

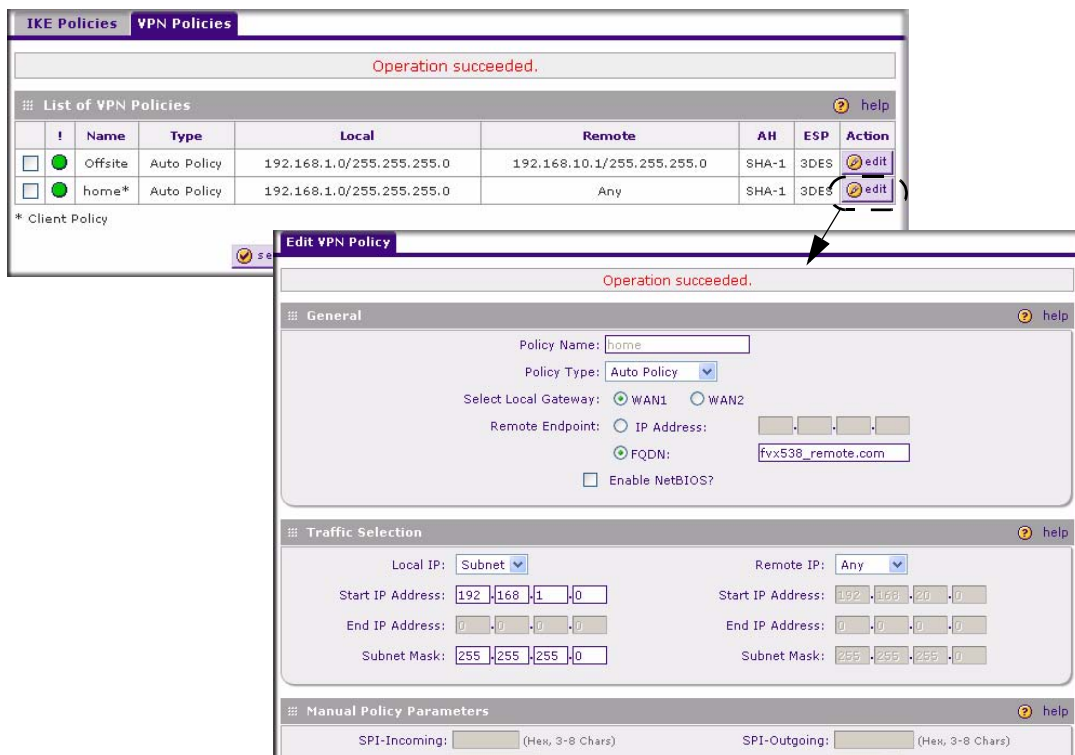


Figure 5-8

You can also view the status of your IKE Policies by clicking the **IKE Policies** tab. The **IKE Policies** screen will display. Then view or edit the parameters of the “Home” policy by clicking **Edit** in the **Action** column adjacent to the policy. The **Edit VPN Policy** screen will display.

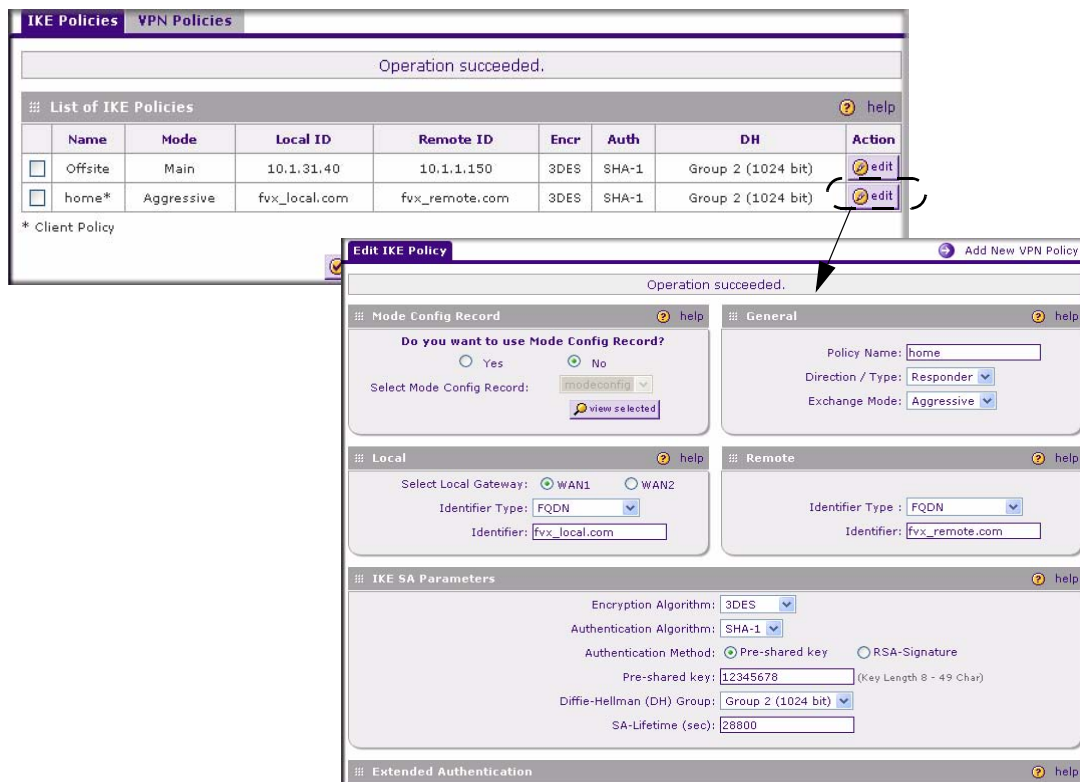


Figure 5-9

VPN Tunnel Policies

When you use the VPN Wizard to set up a VPN tunnel, both a VPN Policy and an IKE Policy are established and populated in both Policy Tables. The name you selected as the VPN Tunnel connection name during Wizard setup identifies both the VPN Policy and IKE Policy. You can edit existing policies, or add new VPN and IKE policies directly in the Policy Tables.

IKE Policy

The IKE (Internet Key Exchange) protocol performs negotiations between the two VPN Gateways, and provides automatic management of the Keys used in IPsec. It is important to remember that:

- “Auto” generated VPN policies must use the IKE negotiation protocol.

- “Manual” generated VPN policies cannot use the IKE negotiation protocol.

Managing IKE Policies

IKE Policies are activated when:

1. The VPN Policy Selector determines that some traffic matches an existing VPN Policy. If the VPN policy is of type “Auto”, then the **Auto Policy Parameters** defined in the VPN Policy are accessed which specify which IKE Policy to use.
2. If the VPN Policy is a “Manual” policy, then the **Manual Policy Parameters** defined in the VPN Policy are accessed and the first matching IKE Policy is used to start negotiations with the remote VPN Gateway.
 - If negotiations fail, the next matching IKE Policy is used.
 - If none of the matching IKE Policies are acceptable to the remote VPN Gateway, then a VPN tunnel cannot be established.
3. An IKE session is established, using the SA (Security Association) parameters specified in a matching IKE Policy:
 - Keys and other parameters are exchanged.
 - An IPSec SA (Security Association) is established, using the parameters in the VPN Policy.

The VPN tunnel is then available for data transfer.

IKE Policy Table

When you use the VPN Wizard to set up a VPN tunnel, an IKE Policy is established and populated in the Policy Table and is given the same name as the new VPN connection name. You can also edit exiting policies or add new IKE policies directly on the Policy Table Screen. Each policy contains the following data:

- **Name.** Uniquely identifies each IKE policy. The name is chosen by you and used for the purpose of managing your policies; it is not supplied to the remote VPN Server.
- **Mode.** Two modes are available: either “Main” or “Aggressive”.
 - Main Mode is slower but more secure.
 - Aggressive mode is faster but less secure. (If specifying either a FQDN or a User FQDN name as the Local ID/Remote ID, aggressive mode is automatically selected.)
- **Local ID.** The IKE/ISAKMP identify of this device. (The remote VPN must have this value as their “Remote ID”.)

- **Remote ID.** The IKE/ISAKMP identify of the remote VPN Gateway. (The remote VPN must have this value as their “Local ID”.)
- **Encr.** Encryption Algorithm used for the IKE SA. The default setting using the VPN Wizard is 3DES. (This setting must match the Remote VPN.)
- **Auth.** Authentication Algorithm used for the IKE SA. The default setting using the VPN Wizard is SHA1. (This setting must match the Remote VPN.)
- **DH.** Diffie-Hellman Group. The Diffie-Hellman algorithm is used when exchanging keys. The DH Group sets the number of bits. The VPN Wizard default setting is Group 2. (This setting must match the Remote VPN.)

To gain a more complete understanding of the encryption, authentication and DH algorithm technologies, see [Appendix B, “Related Documents”](#) for a link to the NETGEAR website.

VPN Policy

You can create two types of VPN Policies. When using the VPN Wizard to create a VPN policy, only the Auto method is available.

- **Manual.** All settings (including the keys) for the VPN tunnel are manually input at each end (both VPN Endpoints). No third party server or organization is involved.
- **Auto.** Some parameters for the VPN tunnel are generated automatically by using the IKE (Internet Key Exchange) protocol to perform negotiations between the two VPN Endpoints (the Local ID Endpoint and the Remote ID Endpoint).

In addition, a CA (Certificate Authority) can also be used to perform authentication (see [“Certificate Authorities” on page 5-27](#)). To use a CA, each VPN Gateway must have a Certificate from the CA. For each Certificate, there is both a “Public Key” and a “Private Key”. The “Public Key” is freely distributed, and is used to encrypt data. The receiver then uses their “Private Key” to decrypt the data (without the Private Key, decryption is impossible). CAs can be beneficial since using them reduces the amount of data entry required on each VPN Endpoint.

Managing VPN Policies

The VPN Policies screen allows you to add additional policies—either Auto or Manual—and to manage the VPN policies already created. You can edit policies, enable or disable policies, or delete them entirely. The rules for VPN policy use are:

1. Traffic covered by a policy will automatically be sent via a VPN tunnel.
2. When traffic is covered by two or more policies, the first matching policy will be used. (In this situation, the order of the policies is important. However, if you have only one policy for each remote VPN Endpoint, then the policy order is not important.)

3. The VPN tunnel is created according to the parameters in the SA (Security Association).
4. The remote VPN Endpoint must have a matching SA, or it will refuse the connection.

VPN Policy Table

Only one Client Policy may be configured at a time (noted by an “*” next to the policy name). The Policy Table contains the following fields:

- **! (Status).** Indicates whether the policy is enabled (green circle) or disabled (grey circle). To Enable or Disable a Policy, check the radio box adjacent to the circle and click **Enable** or **Disable**, as required.
- **Name.** Each policy is given a unique name (the Connection Name when using the VPN Wizard).
- **Type.** The Type is “Auto” or “Manual” as described previously (Auto is used during VPN Wizard configuration).
- **Local.** IP address (either a single address, range of address or subnet address) on your local LAN. Traffic must be from (or to) these addresses to be covered by this policy. (The Subnet address is supplied as the default IP address when using the VPN Wizard).
- **Remote.** IP address or address range of the remote network. Traffic must be to (or from) these addresses to be covered by this policy. (The VPN Wizard default requires the remote LAN IP address and subnet mask).
- **AH.** Authentication Header. This specifies the authentication protocol for the VPN header (VPN Wizard default is disabled).
- **ESP.** Encapsulating Security Payload. This specifies the encryption protocol used for the VPN data (VPN Wizard default is enabled).
- **Action.** Allows you to access individual policies to make any changes or modifications.

VPN Tunnel Connection Status

Recent VPN tunnel activity is shown on the **IPSec Connection Status** screen (accessed by selecting **VPN** from the main menu and **Connection Status** from the submenu). You can set a Poll Interval (in seconds) to check the connection status of all active IKE Policies to obtain the latest VPN tunnel activity. The Active IPSec (SA)s table also lists current data for each active IPSec SA (Security Association):

- **Policy Name.** The name of the VPN policy associated with this SA.
- **Endpoint.** The IP address on the remote VPN Endpoint.

- **Tx (KBytes).** The amount of data transmitted over this SA.
- **Tx (Packets).** The number of packets transmitted over this SA.
- **State.** The current state of the SA. Phase 1 is “Authentication phase” and Phase 2 is “Key Exchange phase”.
- **Action.** Allows you to terminate or build the SA (connection), if required.

Creating a VPN Gateway Connection: Between FVX538 and FVS338

This section describes how to configure a VPN connection between a NETGEAR FVX538 VPN Firewall and a NETGEAR FVS338 VPN Firewall.

Using the VPN Wizard for each VPN firewall, we will create a set of policies (IKE and VPN) that will allow the two firewalls to connect from locations with fixed IP addresses. Either firewall can initiate the connection.

This procedure was developed using:

- Netgear FVX538 VPN Firewall
 - WAN1 IP address is 10.1.32.40
 - LAN IP address subnet is 192.168.1.1/255.255.255.0
- Netgear FVS338 VPN Firewall (remote gateway)
 - WAN IP address is 10.1.1.150
 - LAN IP address subnet is 192.168.2.1/255.255.255.0

Configuring the FVX538

To configure the FVX538 VPN Wizard:

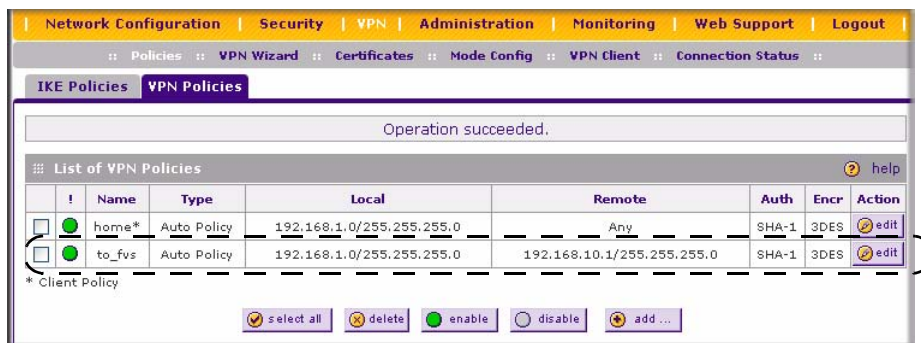
1. Select **VPN** from the main menu. The **Policies** submenu will display showing the **IKE Policies** screen
2. Select **VPN Wizard**. The **VPN Wizard** screen will display.
3. Select the **VPN Tunnel** connection type; in this case, the Gateway radio box is selected.
4. Give the client connection a name, such as **to_fvs**.
5. Enter a value for the pre-shared key.

- Select the local WAN interface to bind this connection to the WAN port for the VPN tunnel.

The screenshot displays the VPN Wizard configuration interface. At the top, there is a navigation bar with tabs for Network Configuration, Security, VPN, Administration, Monitoring, Web Support, and Logout. Below this, the breadcrumb trail shows Policies > VPN Wizard > Certificates > Mode Config > VPN Client > Connection Status. The main title is 'VPN Wizard' with a sub-header 'VPN Wizard Default Values'. The 'About VPN Wizard' section contains introductory text and a note that the VPN tunnel will connect to Gateway peers. The 'Connection Name and Remote IP Type' section includes input fields for 'to_fvs' as the connection name and '12345678' as the pre-shared key, with 'WAN 1' selected as the local interface. The 'End Point Information' section has input fields for remote WAN IP '10.1.1.150' and local WAN IP '10.1.31.40'. The 'Secure Connection Remote Accessibility' section features segmented input fields for remote LAN IP '192.168.2.1' and subnet mask '255.255.255.0'. 'Apply' and 'Reset' buttons are located at the bottom of the form.

Figure 5-10

- Enter the WAN IP address of the remote FVS338 and then enter the WAN IP address of the local FVX538. (Both local and remote ends must define the address as either an IP address or a FQDN. A combination of IP address and FQDN is not permissible.)
- Enter the LAN IP address and subnet mask of the remote FVS338.
- Click **Apply** to create the “to_fvs” IKE and VPN policies. The VPN Policies screen will display showing the “to_fvs” policy as enabled in the **List of VPN Policies** table.

**Figure 5-11**

To view the VPN Policy parameters:

1. Click **Edit** in the **Action** column adjacent to the “to_fvs” policy. The **Edit VPN Policy** screen will display. (It should not be necessary to make any changes.)
2. View the IKE Policy statistics associated with this policy by clicking **View Selected**.

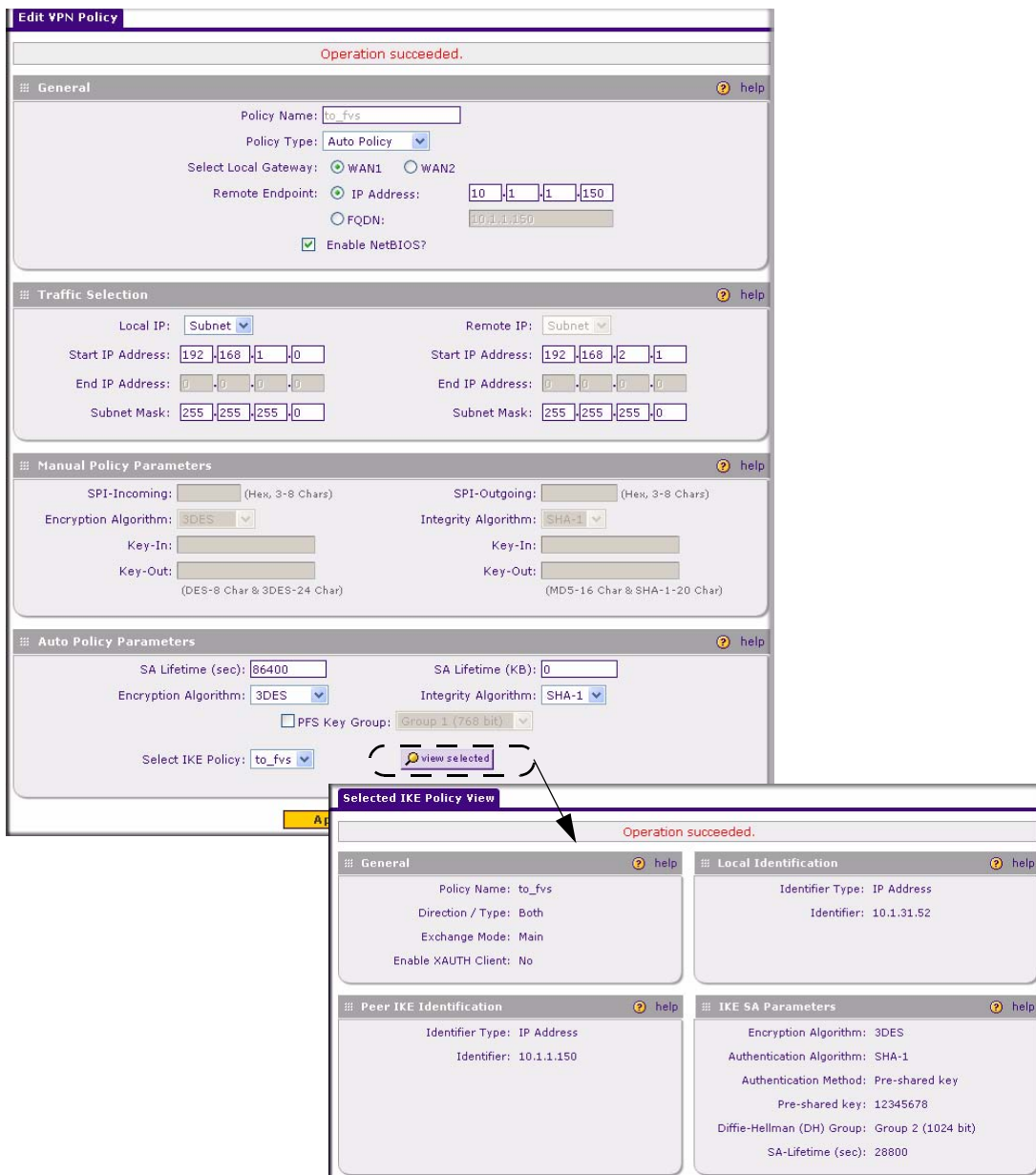


Figure 5-12

To view the IKE Policy Configuration parameters:

1. Select the **IKE Policies** tab. The **IKE Policies** table will display.

2. Select “to_FVS” and click **Edit**. It should not be necessary to make any changes)

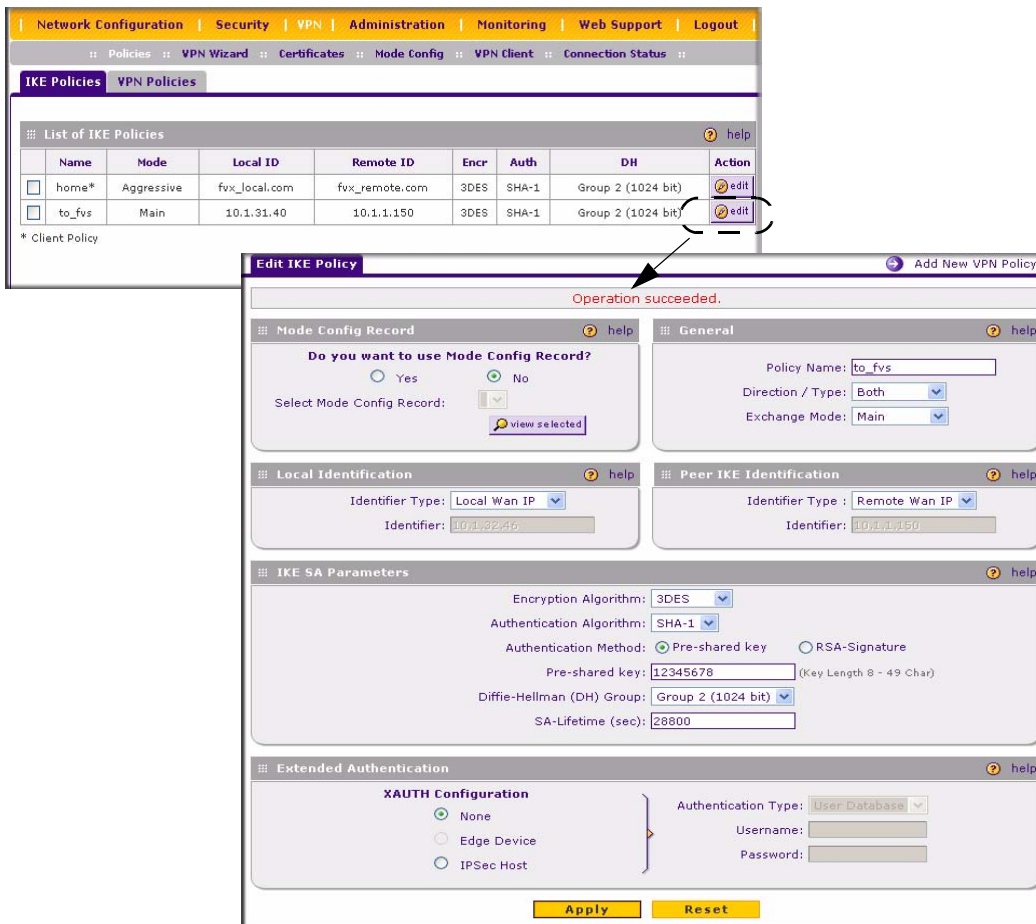



Figure 5-13

 **Note:** When XAUTH is enabled as an Edge Device, incoming VPN connections are authenticated against the FVX538 User Database first; then, if configured, a RADIUS server is checked. If IPSec Host is enabled, users are authenticated by the remote host.

Configuring the FVS338

To configure the FVS338 VPN Wizard:

1. Select **VPN** from the main menu and **VPN Wizard** from the submenu. The **VPN Wizard** screen will display.
2. Check the **Gateway** radio box for the type of VPN tunnel connection.
3. Give the new connection a name, such as **to_fvx..**

Figure 5-14

4. Enter a value for the pre-shared key.
5. Enter the WAN IP address of the remote FVX538.
6. Enter the WAN IP address of the FVS338.
7. Enter the LAN IP address and subnet mask of the remote FVX538.

8. Click **Apply** to create the “to_fvx” IKE and VPN policies. The **VPN Policies** screen will display.

Testing the Connection

To test the VPN gateway tunnel:

1. From a PC on either LAN firewall, try to ping a PC on the LAN of the other firewall. Establishing the VPN connection may take several seconds.
2. For additional status and troubleshooting information, view VPN Logs and VPN Connections Status screens in the FVX538 or FVS338.

Creating a VPN Client Connection: VPN Client to FVX538

This section describes how to configure a VPN connection between a Windows PC and the VPN firewall.

Using the FVX538's VPN Wizard, we will create a single set of VPN Client policies (IKE and VPN) that will allow up to 200 remote PCs to connect from locations in which their IP addresses are unknown in advance. The PCs may be directly connected to the Internet or may be behind NAT routers. If more PCs are to be connected, an additional policy or policies must be created.

Each PC will use Netgear's ProSafe VPN Client software. Since the PC's IP address is assumed to be unknown, the PC must always be the Initiator of the connection.

This procedure was developed and tested using:

- Netgear ProSafe VPN Firewall 200
- Netgear ProSafe VPN Client
- NAT router: Netgear FR114P

Configuring the FVX538

1. Select the VPN Wizard.
2. Select the **VPN Client** radio button for type of VPN connection.
3. Give the client connection a name, such as “home”.
4. Enter a value for the pre-shared key.

5. Check either the WAN1 or WAN 2 radio box to select the WAN interface tunnel.

The screenshot shows the VPN Wizard configuration page. The navigation bar includes: Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout. The breadcrumb trail is: Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status. The main content area is titled 'VPN Wizard' and includes a 'VPN Wizard Default Values' link. The 'About VPN Wizard' section states: 'The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPN), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the Policies menu.' Below this, it says 'This VPN tunnel will connect to the following peers:' with radio buttons for 'Gateway' and 'VPN Client' (selected). The 'Connection Name and Remote IP Type' section has input fields for 'What is the new Connection Name?' (home), 'What is the pre-shared key?' (12345678), and 'This VPN tunnel will use following local WAN Interface:' (WAN 1 selected, WAN 2 unselected). The 'End Point Information' section has input fields for 'What is the Remote Identifier Information?' (fvx_remote.com) and 'What is the Local Identifier Information?' (fvx_local.com). The 'Secure Connection Remote Accessibility' section has input fields for 'What is the remote LAN IP Address?' and 'What is the remote LAN Subnet Mask?'. At the bottom are 'Apply' and 'Reset' buttons.

Figure 5-15


6. Enter the remote WAN's IP Address or Internet Name and then enter the local WAN's IP Address or Internet Name. In this example, we are using their FQDNs. (Both the local and remote addresses must be of the same type—either both must be FQDN or both must be an IP address.)
7. Click **Apply** to create the “home” VPN Client. The **VPN Policies** screen will display showing the VPN Client policy as enabled.
8. Click the **IKE Policies** tab to display the **IKE Policies** table and click **Edit** adjacent to the “home” policy to view the “home” policy details.

You can also augment user authentication security by enabling the XAUTH server by selecting the **Edge Device** radio box and then adding users to the User Database (see [“Extended Authentication \(XAUTH\) Configuration”](#) on page 5-31 and [“User Database Configuration”](#) on page 5-34, respectively). Alternatively, you can also choose to selection either a RADIUS-CHAP or RADIUS-PAP server.

Configuring the VPN Client

From a PC with the Netgear Prosafe VPN Client installed, you can configure a VPN client policy to connect to the FVX538.

To configure your VPN client:

1. Right-click on the VPN client icon  in your Windows toolbar and select **Security Policy Editor**.
2. In the upper left of the Policy Editor window, click the New Document icon to open a New Connection. Give the New Connection a name, such as **to_FVX**.

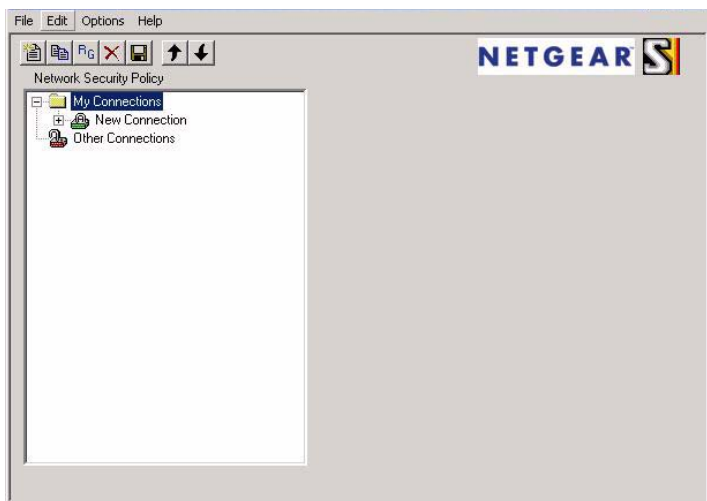


Figure 5-16

3. From the **ID Type** pull-down menu, select **IP Subnet**.
4. Enter the LAN **IP Subnet Address** and **Subnet Mask** of the FVX538 LAN. Check the **Connect using** radio box and select **Secure Gateway Tunnel** from the pull-down menu.
5. From the first **ID Type** pull-down menus, select **Domain Name** and enter the FQDN address of the FVX538.
6. From the second **ID Type** pull-down menu, select **Gateway IP Address** and enter the WAN IP Gateway address of the FVX538.

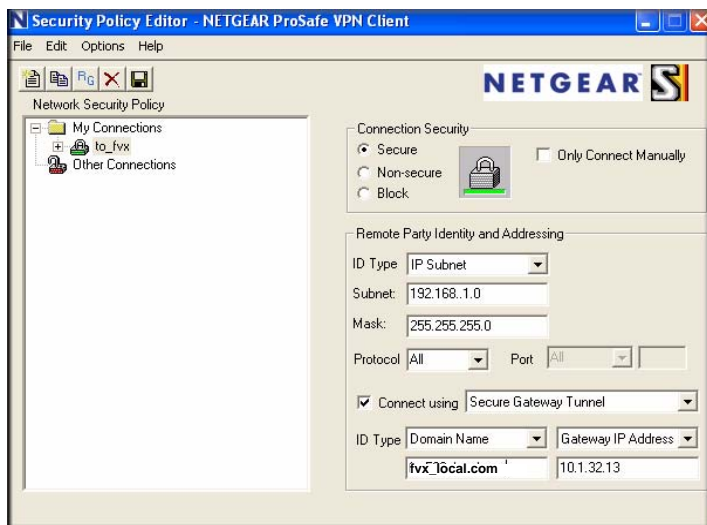


Figure 5-17

7. In the left frame, click **My Identity**.
8. From the **Select Certificate** pull-down menu, select **None**.
9. From the ID Type pull-down menu, select **Domain Name**.

The value entered under Domain Name will be of the form “<name><XY>.fvx_remote.com”, where each user must use a different variation on the Domain Name entered here. The <name> is the policy name used in the FVX538 configuration. In this example, it is “home”. X and Y are an arbitrary pair of numbers chosen for each user.

	Note: X may not be zero!
---	---------------------------------

In this example, we have entered **home11.fvx_remote.com**. Up to 200 user variations can be served by one policy.

10. Leave **Virtual Adapter** disabled, and select your computer’s Network Adapter. Your current IP address will appear.

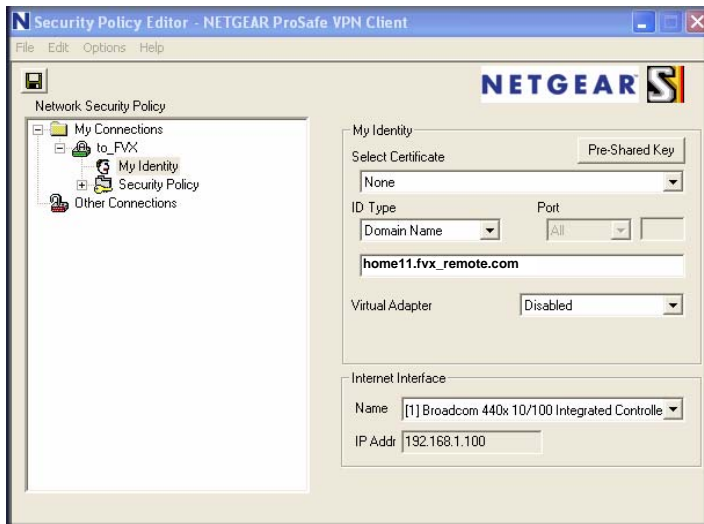


Figure 5-18

5. Before leaving the My Identity menu, click **Pre-Shared Key**.
6. Click **Enter Key** and then enter your preshared key, and click **OK**. This key will be shared by all users of the FVX538 policy “home”.

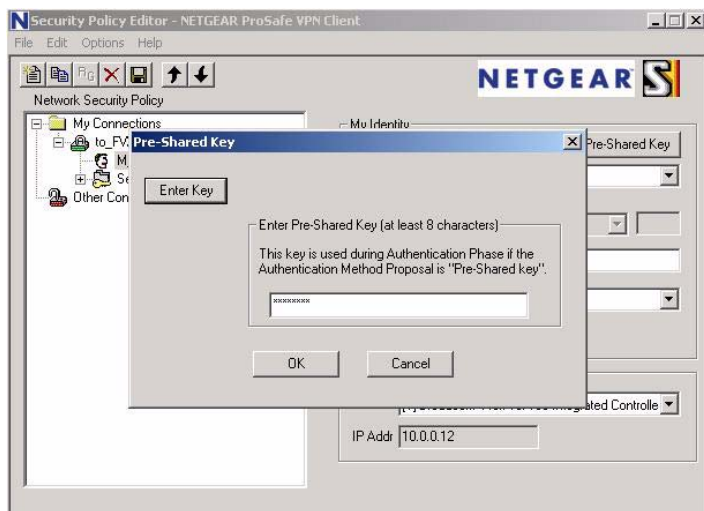


Figure 5-19

7. In the left frame, select **Security Policy**.

8. For the **Phase 1 Negotiation Mode**, check the **Aggressive Mode** radio box.
9. **PFS** should be disabled, and **Enable Replay Detection** should be enabled.

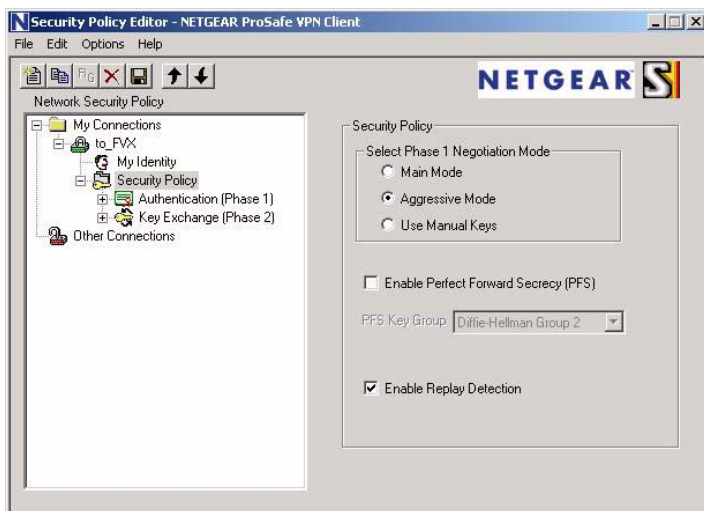


Figure 5-20

10. In the left frame, expand **Authentication (Phase 1)** and select **Proposal 1**. The Proposal 1 fields should mirror those in the following figure. No changes should be necessary.

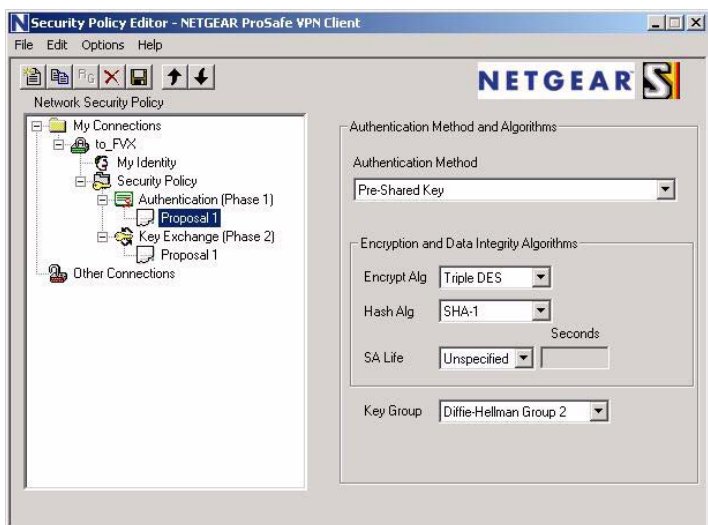


Figure 5-21

11. In the left frame, expand **Key Exchange (Phase 2)** and select **Proposal 1**. The fields in this proposal should also mirror those in the following figure. No changes should be necessary.
12. In the upper left of the window, click the disk icon to save the policy.

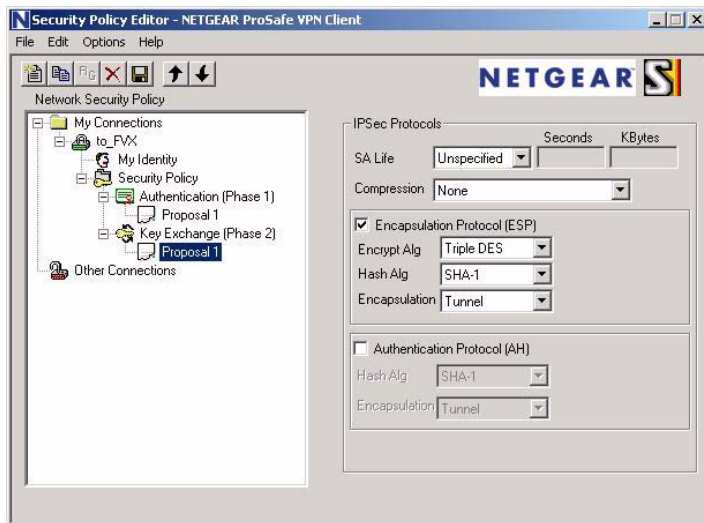




Figure 5-22

Testing the Connection

1. From your PC, right-click on the VPN client icon  in your Windows toolbar and select **Connect...**, then **My Connections\to_FVX**.

Within 30 seconds you should receive the message “Successfully connected to My Connections\to_FVX” and the VPN client icon in the toolbar should say On: .

- For additional status and troubleshooting information, right-click on the VPN client icon Logs and Connection Status screens in the FVX538.

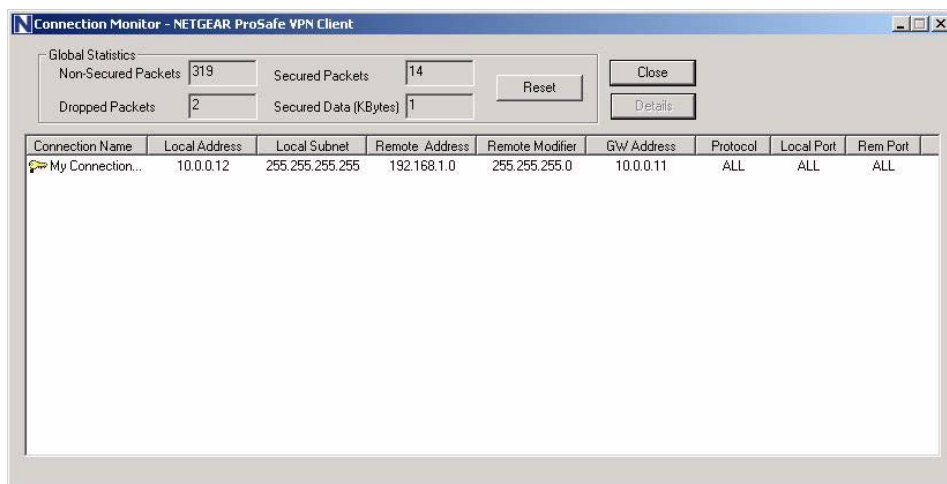


Figure 5-23

Certificate Authorities

Digital Self Certificates are used to authenticate the identity of users and systems, and are issued by various CAs (Certification Authorities). Digital Certificates are used by this router during the IKE (Internet Key Exchange) authentication phase as an alternative authentication method. Self Certificates are issued to you by various CAs (Certification Authorities).

Each CA also issues a CA Identity certificate shown in the **Trusted Certificates (CA Certificates)** table. This Certificate is required in order to validate communication with the CA. It is a three-step process. First, you generate a CA request; then, when the request is granted, you upload the Self Certificate (shown in the **Active Self Certificates** table) and then you upload the CA Identity certificate (shown in the **Trusted Certificates** table).

The **Trusted Certificates** table lists the certificates generated and signed by a publicly known organization or authority called the Certificate Authority. The table lists the certificates of each CA and contains the following data:

- CA Identity (Subject Name).** The organization or person to whom the certificate is issued.
- Issuer Name.** The name of the CA that issued the certificate.
- Expiry Time.** The date after which the certificate becomes invalid

The Active Self Certificates table shows the Certificates issued to you by the various CAs (Certification Authorities), and available for use. For each Certificate, the following data is listed:

- **Name.** The name you used to identify this Certificate.
- **Subject Name.** This is the name which other organizations will see as the Holder (owner) of this Certificate. This should be your registered business name or official company name. Generally, all Certificates should have the same value in the Subject field.
- **Serial Number.** It is a serial number maintained by the CA. It is used to identify the certificate with in the CA.
- **Issuer Name.** The name of the CA which issued the Certificate.
- **Expiry Time.** The date on which the Certificate expires. You should renew the Certificate before it expires.

Generating a Self Certificate Request

To use a Certificate, you must first request the certificate from the CA, then download and activate the certificate on your system.

To request a Certificate from the CA:

1. From the main menu under **VPN**, select the **Certificates** submenu. The Certificates screen will display.
2. In the **Generate Self Certificate Request**, enter the required data:
 - **Name** – Enter a name that will identify this Certificate.
 - **Subject** – This is the name which other organizations will see as the Holder (owner) of the Certificate. Since this name will be seen by other organizations, you should use your registered business name or official company name. (Using the same name, or a derivation of the name, in the Title field would be useful.)
 - From the pull-down menus, select the following values:
 - Hash Algorithm: MD5 or SHA2.
 - Signature Algorithm: RSA.
 - Signature Key Length: 512, 1024, 2048. (Larger key sizes may improve security, but may also impact performance.)
3. Complete the Optional fields, if desired, with the following information:
 - **IP Address** – If you have a fixed IP address, you may enter it here. Otherwise, you should leave this field blank.

Operation succeeded.

Trusted Certificates (CA Certificate) help

CA Identity (Subject Name)	Issuer Name	Expiry Time
<input checked="" type="checkbox"/> select all <input type="checkbox"/> delete		

Upload Trusted Certificate:

Trusted Certificate File: Browse...

Active Self Certificates help

Name	Subject Name	Serial Number	Issuer Name	Expiry Time
<input checked="" type="checkbox"/> select all <input type="checkbox"/> delete				

Generate Self Certificate Request help

Name:

Subject:

Hash Algorithm:

Signature Algorithm:

Signature Key Length:

IP Address (Optional):

Domain Name (Optional):

E-mail Address (Optional):

Self Certificate Requests help

Name	Status	Action
<input type="checkbox"/> NETGEAR	0	<input type="button" value="view"/>
<input checked="" type="checkbox"/> select all <input type="checkbox"/> delete		

Upload certificate corresponding to a request above:

Certificate File: Browse...

Figure 5-24

- **Domain Name** – If you have a Domain name, you can enter it here. Otherwise, you should leave this field blank.
 - **E-mail Address** – Enter your e-mail address in this field.
4. Click **Generate**. A new certificate request is created and added to the **Self Certificate requests** table.
 5. Click **View** under the **Action** column to view the request.

6. Copy the contents of the **Data to supply to CA** text box into a file, including all of the data contained in “---BEGIN CERTIFICATE REQUEST---” and “---END CERTIFICATE REQUEST---”. Click **Done**. You will return to the Certificate screen and your Request details will be displayed in the **Self Certificates Requests** table showing a Status of “Waiting for Certificate upload”

To submit your Certificate request to a CA:

1. Connect to the Website of the CA.
2. Start the Self Certificate request procedure.
3. When prompted for the requested data, copy the data from your saved data file (including “---BEGIN CERTIFICATE REQUEST---” and “---END CERTIFICATE REQUEST”).
4. Submit the CA form. If no problems ensue, the Certificate will be issued.

Uploading a Trusted Certificate

After obtaining a new Certificate from the CA, you must upload the certificate to this device and add it to your Trusted Certificates:

To upload your new certificate:

1. From the main menu, under **VPN**, select **Certificates**. The Certificates screen will display. Scroll down to the **Self Certificate Requests** section.
2. Click **Browse**, and locate the certificate file on your PC. Select the file name in the “File to upload” field and click **Upload**. The certificate file will be uploaded to this device.
3. Scroll back to the **Active Self Certificates** table. The new Certificate will appear in the **Active Self Certificates** list.

Certificates are updated by their issuing CA authority on a regular basis. You should track all of your CAs to ensure that you have the latest version and/or that your certificate has not been revoked. To track your CAs, you must upload the Certificate Identify for each CA to the CRL.

Managing your Certificate Revocation List (CRL)

CRL (Certificate Revocation List) files show Certificates which are active and certificates which have been revoked, and are no longer valid. Each CA issues their own CRLs.

It is important that you keep your CRLs up-to-date. You should obtain the CRL for each CA regularly.

The CRL table lists your active CAs and their critical release dates:

- CA Identify – The official name of the CA which issued this CRL.
- Last Update – The date when this CRL was released.
- Next Update – The date when the next CRL will be released.

To upload a Certificate Identify to the CRL:

1. From the main menu under VPN, select **Certificates**. The **Certificates** screen will display showing the CRL (Certificate Revocation List) table at the bottom of the screen.
2. Click **Browse**, and then locate the file you previously downloaded from a CA.
3. Select the Certificate Identify file. The name will appear in the “File to upload” field. Click **Upload**.

Click **Back** to return to the CRL list. The new Certificate Identify will appear in the CRL Table. If you have a previous CA Identity from the same CA, it should now be deleted.



Figure 5-25

Extended Authentication (XAUTH) Configuration

When connecting many VPN clients to a VPN gateway router, an administrator may want a unique user authentication method beyond relying on a single common preshared key for all clients. Although the administrator could configure a unique VPN policy for each user, it is more convenient for the VPN gateway router to authenticate users from a stored list of user accounts. XAUTH provides the mechanism for requesting individual authentication information from the user, and a local User Database or an external authentication server, such as a RADIUS server, provides a method for storing the authentication information centrally in the local network.

XAUTH is enabled when adding or editing an IKE Policy. Two types of XAUTH are available:

- **Edge Device.** If this is selected, the router is used as a VPN concentrator where one or more gateway tunnels terminate. If this option is chosen, you must specify the authentication type to be used in verifying credentials of the remote VPN gateways: User Database, RADIUS-PAP, or RADIUS-CHAP.

- **IPSec Host.** If you want authentication by the remote gateway, enter a User Name and Password to be associated with this IKE policy. If this option is chosen, the remote gateway must specify the user name and password used for authenticating this gateway.



Note: If a RADIUS-PAP server is enabled for authentication, XAUTH will first check the local User Database for the user credentials. If the user account is not present, the router will then connect to a RADIUS server.

Configuring XAUTH for VPN Clients

Once the XAUTH has been enabled, you must establish user accounts on the Local Database to be authenticated against XAUTH, or you must enable a RADIUS-CHAP or RADIUS-PAP server.



Note: If you are modifying an existing IKE Policy to add **XAUTH**, if it is in use by a VPN Policy, the VPN policy must be disabled before you can modify the IKE Policy.

To enable and configure XAUTH:

1. Select **VPN** from the main menu and **Policies** from the submenu. The **IKE Policies** screen will display.
2. You can add **XAUTH** to an existing IKE Policy by clicking **Edit** adjacent to the policy to be modified or you can create a new IKE Policy incorporating **XAUTH** by clicking **Add**.
3. In the **Extended Authentication** section check the **Edge Device** radio box to use this router as a VPN concentrator where one or more gateway tunnels terminate. You then must specify the authentication type to be used in verifying credentials of the remote VPN gateways. (Either the User Database or RADIUS Client must be configured when XAUTH is enabled.)
4. In the **Extended Authentication** section, select the **Authentication Type** from the pull-down menu which will be used to verify user account information. Select
 - **Edge Device** to use this router as a VPN concentrator where one or more gateway tunnels terminate. When this option is chosen, you will need to specify the authentication type to be used in verifying credentials of the remote VPN gateways.
 - **User Database** to verify against the router's user database. Users must be added through the User Database screen (see [“User Database Configuration”](#) on page 5-34).

- **RADIUS-CHAP** or **RADIUS-PAP** (depending on the authentication mode accepted by the RADIUS server) to add a RADIUS server. If RADIUS-PAP is selected, the router will first check in the User Database to see if the user credentials are available. If the user account is not present, the router will then connect to the RADIUS server (see “[RADIUS Client Configuration](#)” on page 5-35).
 - **IPSec Host** if you want to be authenticated by the remote gateway. In the adjacent **Username** and **Password** fields, type in the information user name and password associated with the IKE policy for authenticating this gateway (by the remote gateway).
5. Click **Apply** to save your settings.

The screenshot displays the 'Edit IKE Policy' configuration page. At the top, a message indicates 'Operation succeeded.' The page is divided into several sections:

- Mode Config Record:** Includes a 'Do you want to use Mode Config Record?' section with 'Yes' and 'No' radio buttons ('No' is selected), and a 'Select Mode Config Record:' dropdown menu set to 'modeconfig'.
- General:** Contains 'Policy Name:' (to_fvs), 'Direction / Type:' (Both), and 'Exchange Mode:' (Main).
- Local:** Shows 'Select Local Gateway:' (WAN1 selected), 'Identifier Type:' (Local Wan IP), and 'Identifier:' (10.1.1.40).
- Remote:** Shows 'Identifier Type:' (Remote Wan IP) and 'Identifier:' (10.1.1.150).
- IKE SA Parameters:** Includes 'Encryption Algorithm:' (3DES), 'Authentication Algorithm:' (SHA-1), 'Authentication Method:' (Pre-shared key selected), 'Pre-shared key:' (12345678), 'Diffie-Hellman (DH) Group:' (Group 2 (1024 bit)), and 'SA-Lifetime (sec):' (28800).
- Extended Authentication:** Features 'XAUTH Configuration' (None, Edge Device selected, IPSec Host) and 'Authentication Type:' (User Database) with 'Username:' and 'Password:' input fields.

At the bottom of the page are two buttons: **Apply** and **Reset**.

Figure 5-26

User Database Configuration

The **User Database** screen is used to configure and administer users when Extended Authentication is enabled as an Edge Device. Whether or not you use an external RADIUS server, you may want some users to be authenticated locally. These users must be added to the **User Database Configured Users** table.

To add a new user:

1. Select **VPN** from the main menu and **VPN Client** from the submenu. The **User Database** screen will display.
2. Enter a **User Name**. This is the unique ID of a user which will be added to the User Name database.
3. Enter a **Password** for the user, and reenter the password in the **Confirm Password** field.
4. Click **Add**. The User Name will be added to the Configured Users table.

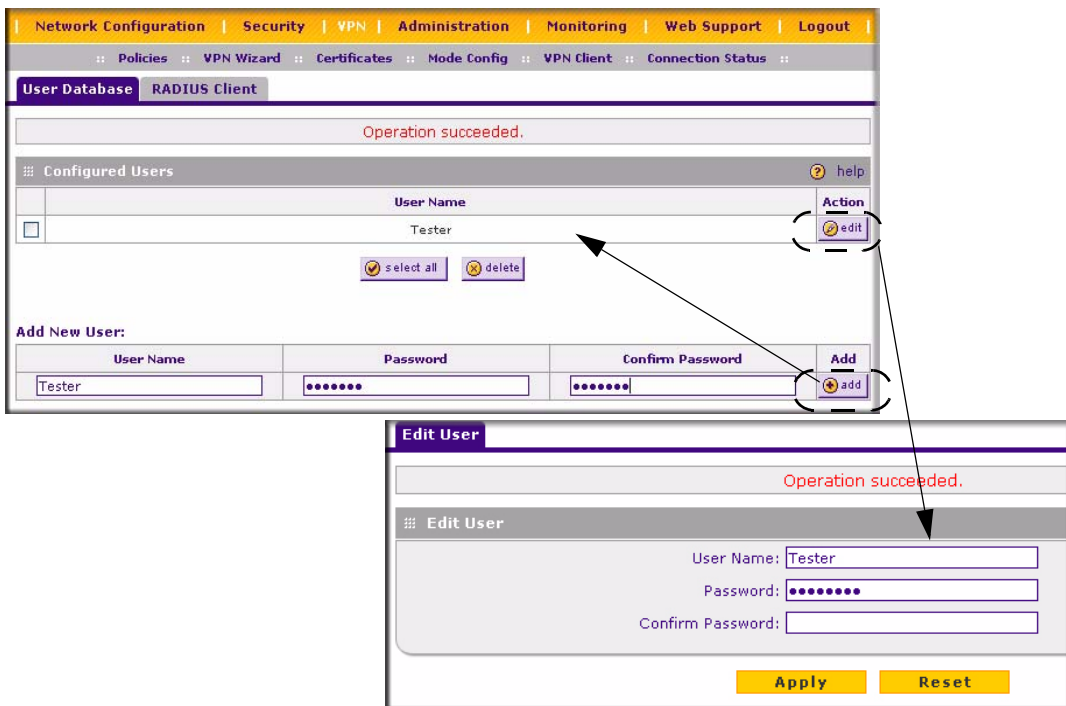


Figure 5-27

To edit the user name or password:

1. Click **Edit** opposite the user's name. The **Edit User** screen will display.
2. Make the required changes to the User Name or Password and click **Apply** to save your settings or **Reset** to cancel your changes and return to the previous settings. The modified user name and password will display in the Configured Users table.

RADIUS Client Configuration

RADIUS (Remote Authentication Dial In User Service, RFC 2865) is a protocol for managing Authentication, Authorization and Accounting (AAA) of multiple users in a network. A RADIUS server will store a database of user information, and can validate a user at the request of a gateway or server in the network when a user requests access to network resources. During the establishment of a VPN connection, the VPN gateway can interrupt the process with an XAUTH (eXtended AUTHentication) request. At that point, the remote user must provide authentication information such as a username/password or some encrypted response using his username/password information. The gateway will try and verify this information first against a local User Database (if RADIUS-PAP is enabled) and then by relaying the information to a central authentication server such as a RADIUS server.

To configure the Primary RADIUS Server:

1. Select **VPN** from the main menu, **VPN Client** from the submenu and then select the **RADIUS Client** tab. The **RADIUS Client** screen will display.
2. Enable the Primary RADIUS server by checking the **Yes** radio box

The screenshot shows the configuration page for the RADIUS Client. The navigation bar at the top includes: Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout. Below this is a breadcrumb trail: Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status. The main content area is titled 'User Database' and 'RADIUS Client'. It is divided into three sections: 1. 'Primary RADIUS Server' with a 'help' icon. It asks 'Do you want to enable a Primary RADIUS Server?' with radio buttons for 'Yes' and 'No' (selected). To the right are input fields for 'Primary Server IP Address', 'Secret Phrase', and 'Primary Server NAS Identifier'. 2. 'Backup RADIUS Server' with a 'help' icon. It asks 'Do you want to enable a Backup RADIUS Server?' with radio buttons for 'Yes' and 'No' (selected). To the right are input fields for 'Backup Server IP Address', 'Secret Phrase', and 'Backup Server NAS Identifier'. 3. 'Connection Configuration' with a 'help' icon. It has input fields for 'Time out period: 30 (Sec)' and 'Maximum Retry Count: 4'. At the bottom are 'Apply' and 'Reset' buttons.

Figure 5-28

3. Enter the **Primary RADIUS Server IP address**.
4. Enter a **Secret Phrase**. Transactions between the client and the RADIUS server are authenticated using a shared secret phrase, so the same Secret Phrase must be configured on both client and server.
5. Enter the **Primary Server NAS Identifier** (Network Access Server). This Identifier **MUST** be present in a RADIUS request. Ensure that NAS Identifier is configured as the same on both client and server.

The FVX538 is acting as a NAS (Network Access Server), allowing network access to external users after verifying their authentication information. In a RADIUS transaction, the NAS must provide some NAS Identifier information to the RADIUS Server. Depending on the configuration of the RADIUS Server, the router's IP address may be sufficient as an identifier, or the Server may require a name, which you would enter here. This name would also be configured on the RADIUS Server, although in some cases it should be left blank on the RADIUS Server.

6. Enable a Backup RADIUS Server (if required) by following steps 2 through 5.
7. Set the **Time Out Period**, in seconds, that the router should wait for a response from the RADIUS server.
8. Set the **Maximum Retry Count**. This is the number of tries the router will make to the RADIUS server before giving up.

9. Click **Reset** to cancel any changes and revert to the previous settings.
10. Click **Apply** to save the settings.



Note: Selection of the Authentication Protocol, usually PAP or CHAP, is configured on the individual IKE policy screens.

Manually Assigning IP Addresses to Remote Users (ModeConfig)

To simplify the process of connecting remote VPN clients to the FVX538, the ModeConfig module can be used to assign IP addresses to remote users, including a network access IP address, subnet mask, and name server addresses from the router. Remote users are given IP addresses available in secured network space so that remote users appear as seamless extensions of the network.

In the following example, we configured the VPN firewall using ModeConfig, and then configured a PC running ProSafe VPN Client software using these IP addresses.

- NETGEAR ProSafe VPN Firewall 200
 - WAN IP address: 172.21.4.1
 - LAN IP address/subnet: 192.168.2.1/255.255.255.0
- NETGEAR ProSafe VPN Client software IP address: 192.168.1.2

Mode Config Operation

After IKE Phase 1 is complete, the VPN connection initiator (remote user/client) asks for IP configuration parameters such as IP address, subnet mask and name server addresses. The Mode Config module will allocate an IP address from the configured IP address pool and will activate a temporary IPSec policy using the template security proposal information configured in the Mode Config record.



Note: After configuring a Mode Config record, you must go to the IKE Policies menu and configure an IKE policy using the newly-created Mode Config record as the Remote Host Configuration Record. The VPN Policies menu does not need to be edited.

Configuring the VPN Firewall

Two menus must be configured—the Mode Config menu and the IKE Policies menu.

To configure the Mode Config menu:

1. From the main menu, select **VPN**, and then select **Mode Config** from the submenu. The **Mode Config** screen will display.
2. Click **Add**. The **Add Mode Config Record** screen will display.
3. Enter a descriptive **Record Name** such as “Sales”.
4. Assign at least one range of IP Pool addresses in the First IP Pool field to give to remote VPN clients.



Note: The IP Pool should not be within your local network IP addresses. Use a different range of private IP addresses such as 172.20.xx.xx.

5. If you have a WINS Server on your local network, enter its IP address.
6. Enter one or two DNS Server IP addresses to be used by remote VPN clients.
7. If you enable Perfect Forward Secrecy (PFS), select DH Group 1 or 2. This setting must match exactly the configuration of the remote VPN client,
8. Specify the Local IP Subnet to which the remote client will have access. Typically, this is your router’s LAN subnet, such as 192.168.2.1/255.255.255.0. (If not specified, it will default to the LAN subnet of the router.)
9. Specify the VPN policy settings. These settings must match the configuration of the remote VPN client. Recommended settings are:
 - SA Lifetime: 3600 seconds
 - Authentication Algorithm: SHA-1
 - Encryption Algorithm: 3DES
10. Click **Apply**. The new record should appear in the VPN Remote Host Mode Config Table (a sample record is shown below).

The image shows two screenshots from a VPN configuration interface. The top screenshot is titled 'Add Mode Config Record' and is divided into two sections: 'Client Pool' and 'Traffic Tunnel Security Level'. The 'Client Pool' section includes fields for 'Record Name' (Sales), 'First IP Pool' (Starting IP 172.20.0.1, Ending IP 172.20.0.99), 'Second IP Pool' (Starting IP 0.0.0.0, Ending IP 0.0.0.0), 'Third IP Pool' (Starting IP 0.0.0.0, Ending IP 0.0.0.0), 'WINS Server' (Primary 10.1.1.7, Secondary 0.0.0.0), and 'DNS Server' (Primary 10.1.1.6, Secondary 0.0.0.0). The 'Traffic Tunnel Security Level' section includes a checked 'PFS Key Group' (Group 2 (1024 bit)), 'SA Lifetime: (sec)' (3600), 'SA Lifetime: (KB)' (0), 'Encryption Algorithm' (3DES), 'Integrity Algorithm' (SHA-1), 'Local IP Address' (192.168.2.1), and 'Local Subnet Mask' (255.255.255.0). 'Apply' and 'Reset' buttons are at the bottom.

The bottom screenshot is titled 'Mode Config' and shows a confirmation message 'Operation succeeded.' followed by a table titled 'List of Mode Config Records'. The table has columns for 'Record Name', 'Pool Star IP', 'Pool End IP', and 'Action'. It lists one record named 'sales' with 'Pool Star IP' 172.20.0.1 and 'Pool End IP' 172.20.0.99. Below the table are buttons for 'select all', 'delete', and 'add ...'.

Record Name	Pool Star IP	Pool End IP	Action
sales	172.20.0.1	172.20.0.99	edit
	0.0.0.0	0.0.0.0	
	0.0.0.0	0.0.0.0	

Figure 5-29

To configure an IKE Policy:

1. From the main menu, select **VPN**. The **IKE Policies** screen will display showing the current policies in the **List of IKE Policies** Table.
2. Click **Add** to configure a new IKE Policy. The **Add IKE Policy** screen will display.
3. Enable **Mode Config** by checking the **Yes** radio box and selecting the Mode Config record you just created from the pull-down menu. (You can view the parameters of the selected record by clicking the **View selected** radio box.)

Mode Config works only in Aggressive Mode, and Aggressive Mode requires that both ends of the tunnel be defined by a FQDN.

4. In the **General** section:
 - a. Enter a description name in the Policy Name Field such as “salesperson”. This name will be used as part of the remote identifier in the VPN client configuration.
 - b. Set Direction/Type to Responder.
 - c. The Exchange Mode will automatically be set to Aggressive.
5. For Local information:
 - d. Select Fully Qualified Domain Name for the Local Identity Type.
 - e. Enter an identifier in the Remote Identity Data field that is not used by any other IKE policies. This identifier will be used as part of the local identifier in the VPN client configuration.
6. Specify the IKE SA parameters. These settings must be matched in the configuration of the remote VPN client. Recommended settings are:
 - Encryption Algorithm: 3DES
 - Authentication Algorithm: SHA-1
 - Diffie-Hellman: Group 2
 - SA Lifetime: 3600 seconds
7. Enter a Pre-Shared Key that will also be configured in the VPN client.
8. XAUTH is disabled by default. To enable XAUTH, select:
 - **Edge Device** to use this router as a VPN concentrator where one or more gateway tunnels terminate. (If selected, you must specify the **Authentication Type** to be used in verifying credentials of the remote VPN gateways.)
 - **IPsec Host** if you want this gateway to be authenticated by the remote gateway. Enter a Username and Password to be associated with the IKE policy. When this option is chosen, you will need to specify the user name and password to be used in authenticating this gateway (by the remote gateway).
9. If Edge Device was enabled, select the **Authentication Type** from the pull down menu which will be used to verify account information: User Database, RADIUS-CHAP or RADIUS-PAP. Users must be added through the User Database screen (see [“User Database Configuration” on page 5-34](#) or [“RADIUS Client Configuration” on page 5-35](#)).



Note: If RADIUS-PAP is selected, the router will first check the User Database to see if the user credentials are available. If the user account is not present, the router will then connect to the RADIUS server.

10. Click **Apply**. The new policy will appear in the IKE Policies Table (a sample policy is shown below)

The screenshot shows the 'Add IKE Policy' configuration window with the following settings:

- Mode Config Record:** Do you want to use Mode Config Record? Yes, No. Select Mode Config Record: sales (view selected).
- General:** Policy Name: salesperson, Direction / Type: Responder, Exchange Mode: Aggressive.
- Local Identification:** Identifier Type: Fqdn, Identifier: local_id.com.
- Peer IKE Identification:** Identifier Type: Fqdn, Identifier: remote_id.com.
- IKE SA Parameters:** Encryption Algorithm: 3DES, Authentication Algorithm: SHA-1, Authentication Method: Pre-shared key, RSA-Signature. Pre-shared key: 12345678 (Key Length 8 - 49 Char). Diffie-Hellman (DH) Group: Group 2 (1024 bit), SA-Lifetime (sec): 28800.
- Extended Authentication:** XAUTH Configuration: None, Edge Device, IPsec Host. Authentication Type: User Database, Username: , Password: .

The 'Apply' button is circled in red. Below it is a smaller window showing the 'List of IKE Policies' table:

Name	Mode	Local ID	Remote ID	Encr	Auth	DH	Action
salesperson	Aggressive	local_id.com	remote_id.com	3DES	SHA-1	Group 2 (1024 bit)	edit

Figure 5-30

Configuring the ProSafe VPN Client for ModeConfig

From a client PC running NETGEAR ProSafe VPN Client software, configure the remote VPN client connection.

To configure the client PC:

1. Right-click the VPN client icon in the Windows toolbar. In the upper left of the Policy Editor window, click the New Policy editor icon.
 - a. Give the connection a descriptive name such as “modecfg_test” (this name will only be used internally).

- b. From the ID Type pull-down menu, select IP Subnet.
- c. Enter the IP Subnet and Mask of the VPN firewall (this is the LAN network IP address of the gateway).
- d. Check the Connect using radio button and select Secure Gateway Tunnel from the pull-down menu.
- e. From the ID Type pull-down menu, select Domain name and enter the FQDN of the VPN firewall; in this example it is “local_id.com”.
- f. Select Gateway IP Address from the second pull-down menu and enter the WAN IP address of the VPN firewall; in this example it is “172.21.4.1”.

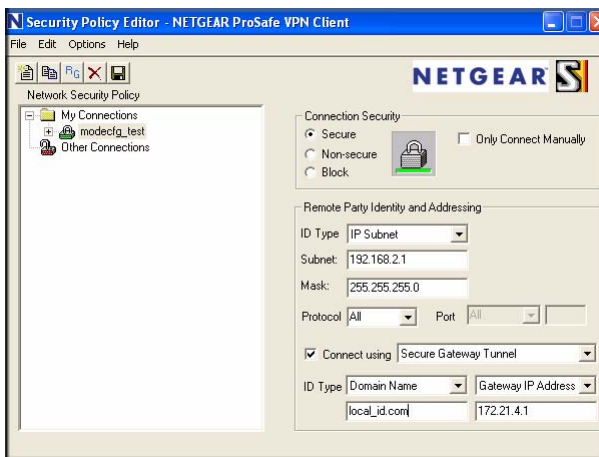


Figure 5-31

2. From the left side of the menu, click My Identity and enter the following information:
 - a. Click **Pre-Shared Key** and enter the key you configured in the FVX538 IKE menu.
 - b. From the Select Certificate pull-down menu, select None.
 - c. From the ID Type pull-down menu, select Domain Name and create an identifier based on the name of the IKE policy you created; for example “salesperson11.remote_id.com”.

- d. Under Virtual Adapter pull-down menu, select Preferred. The Internal Network IP Address should be 0.0.0.0.



Note: If no box is displayed for Internal Network IP Address, go to Options/Global Policy Settings, and check the box for “Allow to Specify Internal Network Address.”

- e. Select your Internet Interface adapter from the Name pull-down menu.

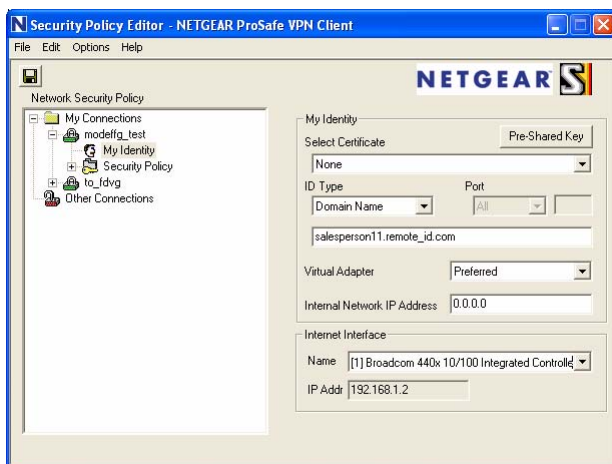


Figure 5-32

3. On the left-side of the menu, select Security Policy.
 - a. Under Security Policy, Phase 1 Negotiation Mode, check the Aggressive Mode radio button.
 - b. Check the Enable Perfect Forward Secrecy (PFS) radio button, and select the Diffie-Hellman Group 2 from the PFS Key Group pull-down menu.
 - c. Enable Replay Detection should be checked.
4. Click on Authentication (Phase 1) on the left-side of the menu and select Proposal 1. Enter the Authentication values to match those in the VPN firewall ModeConfig Record menu.

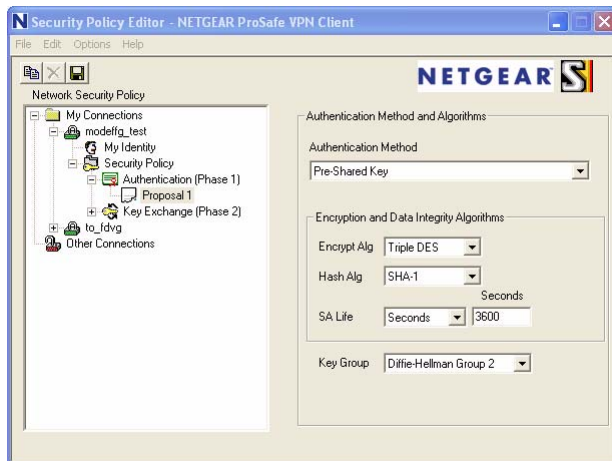


Figure 5-33

- Click on Key Exchange (Phase 2) on the left-side of the menu and select Proposal 1. Enter the values to match your configuration of the VPN firewall ModeConfig Record menu. (The SA Lifetime can be longer, such as 8 hours (28800 seconds)).

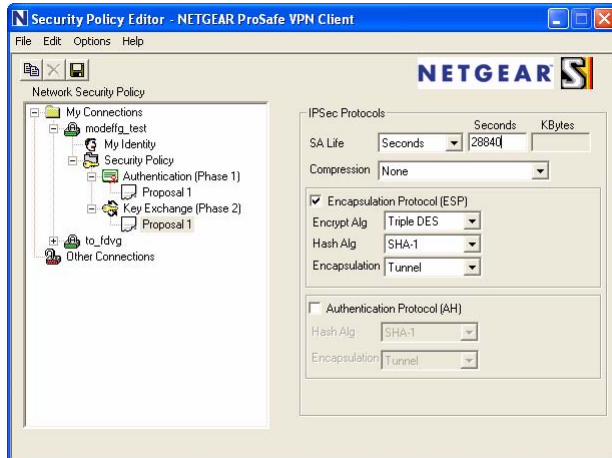


Figure 5-34

- Click the Save icon to save the Security Policy and close the VPN ProSafe VPN client.

To test the connection:

1. Right-click on the VPN client icon in the Windows toolbar and select Connect. The connection policy you configured will appear; in this case “My Connections\modecfg_test”.
2. Click on the connection. Within 30 seconds the message “Successfully connected to MyConnections/modecfg_test will display and the VPN client icon in the toolbar will read “On”.
3. From the client PC, ping a computer on the VPN firewall LAN.

Chapter 6

Router and Network Management

This chapter describes how to use the network management features of your ProSafe VPN Firewall 200. These features can be found by clicking on the appropriate heading in the Main Menu of the browser interface.

The ProSafe VPN Firewall 200 offers many tools for managing the network traffic to optimize its performance. You can also control administrator access, be alerted to important events requiring prompt action, monitor the firewall status, perform diagnostics, and manage the firewall configuration file.

Performance Management

Performance management consists of controlling the traffic through the VPN firewall so that the necessary traffic gets through when there is a bottleneck and either reducing unnecessary traffic or rescheduling some traffic to low-peak times to prevent bottlenecks from occurring in the first place. The VPN firewall has the necessary features and tools to help the network manager accomplish these goals.

Bandwidth Capacity

The maximum bandwidth capacity of the VPN firewall in each direction is as follows:

- LAN side: 1,800 Mbps (eight LAN ports at 100 Mbps each, plus one Gigabit LAN port)
- WAN side: 200 Mbps (load balancing mode, two WAN ports at 100 Mbps each) or 100 Mbps (rollover mode, one active WAN port at 100 Mbps)

In practice, the WAN side bandwidth capacity will be much lower when DSL or cable modems are used to connect to the Internet. At 1.5 Mbps, the WAN ports will support the following traffic rates:

- Load balancing mode: 3 Mbps (two WAN ports at 1.5 Mbps each)
- Rollover mode: 1.5 Mbps (one active WAN port at 1.5 Mbps)

As a result and depending on the traffic being carried, the WAN side of the firewall will be the limiting factor to throughput for most installations.

Using the dual WAN ports in load balancing mode increases the bandwidth capacity of the WAN side of the VPN firewall. But there is no backup in case one of the WAN ports fail. In such an event and with one exception, the traffic that would have been sent on the failed WAN port gets diverted to the WAN port that is still working, thus increasing its loading. The exception is traffic that is bound by protocol to the WAN port that failed. This protocol-bound traffic is not diverted.

VPN Firewall Features That Reduce Traffic

Features of the VPN firewall that can be called upon to decrease WAN-side loading are as follows:

- Service blocking
- Block sites
- Source MAC filtering

Service Blocking

You can control specific outbound traffic (for example, from LAN to WAN and from DMZ to WAN). Outbound Services lists all existing rules for outbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule allows all outgoing traffic.



Warning: This feature is for Advanced Administrators only! Incorrect configuration will cause serious problems.

Each rule lets you specify the desired action for the connections covered by the rule:

- BLOCK always
- BLOCK by schedule, otherwise Allow
- ALLOW always
- ALLOW by schedule, otherwise Block

As you define your firewall rules, you can further refine their application according to the following criteria:

- **LAN Users** – These settings determine which computers on your network are affected by this rule. Select the desired options:
 - Any: All PCs and devices on your LAN.
 - Single address: The rule will be applied to the address of a particular PC.
 - Address range: The rule is applied to a range of addresses.

- **Groups:** The rule is applied to a Group (see [“Managing Groups and Hosts \(LAN Groups\)” on page 3-6](#) to assign PCs to a Group using Network Database).
- **WAN Users** – These settings determine which Internet locations are covered by the rule, based on their IP address.
 - **Any:** The rule applies to all Internet IP address.
 - **Single address:** The rule applies to a single Internet IP address.
 - **Address range:** The rule is applied to a range of Internet IP addresses.
- **Services** – You can specify the desired Services or applications to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see [“Services-Based Rules” on page 4-2](#) and [“Adding Customized Services” on page 4-21](#)).
- **Schedule** – You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see [“Setting a Schedule to Block or Allow Specific Traffic” on page 4-24](#)).

See [“Using Rules to Block or Allow Specific Kinds of Traffic” on page 4-1](#) for the procedure on how to use this feature.

Services. The Rules menu contains a list of predefined Services for creating firewall rules. If a service does not appear in the predefined Services list, you can define the service. The new service will then appear in the Rules menu's Services list.

See [“Services-Based Rules” on page 4-2](#) for the procedure on how to use this feature.

Groups and Hosts. You can apply these rules selectively to groups of PCs to reduce the outbound or inbound traffic. The Network Database is an automatically-maintained list of all known PCs and network devices. PCs and devices become known by the following methods:

- **DHCP Client Request** – By default, the DHCP server in this Router is enabled, and will accept and respond to DHCP client requests from PCs and other network devices. These requests also generate an entry in the Network Database. Because of this, leaving the DHCP Server feature (on the LAN screen) enabled is strongly recommended.
- **Scanning the Network** – The local network is scanned using standard methods such as ARP. This will detect active devices which are not DHCP clients. However, sometimes the name of the PC or device cannot be accurately determined, and will be shown as Unknown.

See [“Managing Groups and Hosts \(LAN Groups\)” on page 3-6](#) for the procedure on how to use this feature.

Schedule. If you have set firewall rules on the Rules screen, you can configure three different schedules (i.e., schedule 1, schedule 2, and schedule 3) for when a rule is to be applied. Once a schedule is configured, it affects all Rules that use this schedule. You specify the days of the week and time of day for each schedule.

See [“Setting a Schedule to Block or Allow Specific Traffic” on page 4-24](#) for the procedure on how to use this feature.

Block Sites

If you want to reduce traffic by preventing access to certain sites on the Internet, you can use the VPN firewall's filtering feature. By default, this feature is disabled; all requested traffic from any Web site is allowed.

- **Keyword (and Domain Name) Blocking** – You can specify up to 32 words that, should they appear in the Web site name (i.e., URL) or in a newsgroup name, will cause that site or newsgroup to be blocked by the VPN firewall.

You can apply the keywords to one or more groups. Requests from the PCs in the groups for which keyword blocking has been enabled will be blocked. Blocking does not occur for the PCs that are in the groups for which keyword blocking has not been enabled.

You can bypass keyword blocking for trusted domains by adding the exact matching domain to the list of Trusted Domains. Access to the domains on this list by PCs even in the groups for which keyword blocking has been enabled will still be allowed without any blocking.

- **Web Component blocking** – You can block the following Web component types: Proxy, Java, ActiveX, and Cookies. Sites on the Trusted Domains list are still subject to Web component blocking when the blocking of a particular Web component has been enabled.

See [“Setting Block Sites \(Content Filtering\)” on page 4-25](#) for the procedure on how to use this feature.

Source MAC Filtering

If you want to reduce outgoing traffic by preventing Internet access by certain PCs on the LAN, you can use the source MAC filtering feature to drop the traffic received from the PCs with the specified MAC addresses. By default, this feature is disabled; all traffic received from PCs with any MAC address is allowed.

See [“Enabling Source MAC Filtering” on page 4-27](#) for the procedure on how to use this feature.

VPN Firewall Features That Increase Traffic

Features that tend to increase WAN-side loading are as follows:

- Port forwarding
- Port triggering
- DMZ port
- Exposed hosts
- VPN tunnels

Port Forwarding

The firewall always blocks DoS (Denial of Service) attacks. A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it (i.e., the service is unavailable). You can also create additional firewall rules that are customized to block or allow specific traffic.



Warning: This feature is for Advanced Administrators only! Incorrect configuration will cause serious problems.

You can control specific inbound traffic (i.e., from WAN to LAN and from WAN to DMZ). Inbound Services lists all existing rules for inbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule blocks all inbound traffic.

Each rule lets you specify the desired action for the connections covered by the rule:

- BLOCK always
- BLOCK by schedule, otherwise Allow
- ALLOW always
- ALLOW by schedule, otherwise Block

You can also enable a check on special rules:

- **VPN Passthrough** – Enable this to pass the VPN traffic without any filtering, specially used when this firewall is between two VPN tunnel end points.
- **Drop fragmented IP packets** – Enable this to drop the fragmented IP packets.
- **UDP Flooding** – Enable this to limit the number of UDP sessions created from one LAN machine.
- **TCP Flooding** – Enable this to protect the router from Syn flood attack.

- **Enable DNS Proxy** – Enable this to allow incoming DNS queries.
- **Enable Stealth Mode** – Enable this to set the firewall to operate in stealth mode.

As you define your firewall rules, you can further refine their application according to the following criteria:

- **LAN Users** – These settings determine which computers on your network are affected by this rule. Select the desired IP Address in this field.
- **WAN Users** – These settings determine which Internet locations are covered by the rule, based on their IP address.
 - Any: The rule applies to all Internet IP address.
 - Single address: The rule applies to a single Internet IP address.
 - Address range: The rule is applied to a range of Internet IP addresses.
- **Destination Address** – These settings determine the destination IP address for this rule which will be applicable to incoming traffic This rule will be applied only when the destination IP address of the incoming packet matches the IP address of the selected WAN interface Selecting ANY enables the rule for any LAN IP destination. WAN1 and WAN2 corresponds to the respective WAN interface governed by this rule.
- **Services** – You can specify the desired Services or applications to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see [“Adding Customized Services” on page 4-21](#)).
- **Schedule** – You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see [“Setting a Schedule to Block or Allow Specific Traffic” on page 4-24](#)).

See [“Using Rules to Block or Allow Specific Kinds of Traffic” on page 4-1](#) for the procedure on how to use this feature.

Port Triggering

Port triggering allows some applications to function correctly that would otherwise be partially blocked by the firewall. Using this feature requires that you know the port numbers used by the Application.

Once configured, Port Triggering operates as follows:

- A PC makes an outgoing connection using a port number defined in the Port Triggering table.
- This Router records this connection, opens the additional INCOMING port or ports associated with this entry in the Port Triggering table, and associates them with the PC.

- The remote system receives the PC's request and responds using the different port numbers that you have now opened.
- This Router matches the response to the previous request and forwards the response to the PC. Without Port Triggering, this response would be treated as a new connection request rather than a response. As such, it would be handled in accordance with the Port Forwarding rules.
 - Only one PC can use a Port Triggering application at any time.
 - After a PC has finished using a Port Triggering application, there is a time-out period before the application can be used by another PC. This is required because the firewall cannot be sure when the application has terminated.

See [“Port Triggering” on page 4-28](#) for the procedure on how to use this feature.

DMZ Port

The DMZ Port allows you to set up the DMZ port. Specifying a Default DMZ Server allows you to set up a computer or server that is available to anyone on the Internet for services that you haven't defined.

The default setting of the rules is that the DMZ port and both inbound and outbound traffic is disabled. Enabling the DMZ port increases the traffic through the WAN ports.

The VPN firewall makes LAN port 8 a dedicated hardware DMZ port when DMZ is enabled (see [“Router Front Panel” on page 1-6](#)).

See [“Configuring and Enabling the DMZ Port” on page 3-10](#) and [“Setting DMZ WAN Rules” on page 4-10](#) for the procedure on how to use this feature.

VPN Tunnels

The VPN firewall permits up to 200 VPN tunnels at a time. Each tunnel requires extensive processing for encryption and authentication.

See [Chapter 5, “Virtual Private Networking”](#) for the procedure on how to use this feature.

Using QoS to Shift the Traffic Mix

The QoS priority settings determine the priority and, in turn, the quality of service for the traffic passing through the firewall. The QoS is set individually for each service.

- You can accept the default priority defined by the service itself by not changing its QoS setting.
- You can change the priority to a higher or lower value than its default setting to give the service higher or lower priority than it otherwise would have.

The QoS priority settings conform to the IEEE 802.1D-1998 (formerly 802.1p) standard for class of service tag.

You will not change the WAN bandwidth used by changing any QoS priority settings. But you will change the mix of traffic through the WAN ports by granting some services a higher priority than others. The quality of a service is impacted by its QoS setting, however.

See [“Setting Quality of Service \(QoS\) Priorities” on page 4-23](#) for the procedure on how to use this feature.

Tools for Traffic Management

The ProSafe VPN Firewall 200 includes several tools that can be used to monitor the traffic conditions of the firewall and control who has access to the Internet and the types of traffic they are allowed to have. See [“Monitoring the Router” on page 6-17](#) for a discussion of the tools.

Administration

You can change the administrator and guest passwords and settings, configure an SNMP manager, backup settings and upgrade firmware, and enable remote management. Administrator access is read/write and guest access is read-only.


Changing Passwords and Settings

The default passwords for the firewall’s Web Configuration Manager is **password**. Netgear recommends that you change this password to a more secure password. You can also configure a separate password for guests.

To modify User or Admin settings:

1. Select **Administration** from the main menu and **Set Password** from the submenu. The **Set Password** screen will display.
2. Select the Settings you wish to edit by checking either the **Edit Admin Settings** or **Edit Guest Settings** radio box.
3. Change the password by first entering the old password, and then entering the new password twice.
4. Click **Apply** to save your settings or **Cancel** to return to your previous settings.
5. Change the **Idle Logout Time** field to the number of minutes you require. The default is 5 minutes.

6. Click **Apply** to save this setting..

 **Note:** If you make the administrator login time-out value too large, you will have to wait a long time before you are able to log back into the router if your previous login was disrupted (i.e., you did not click **Logout** on the Main Menu bar to log out).

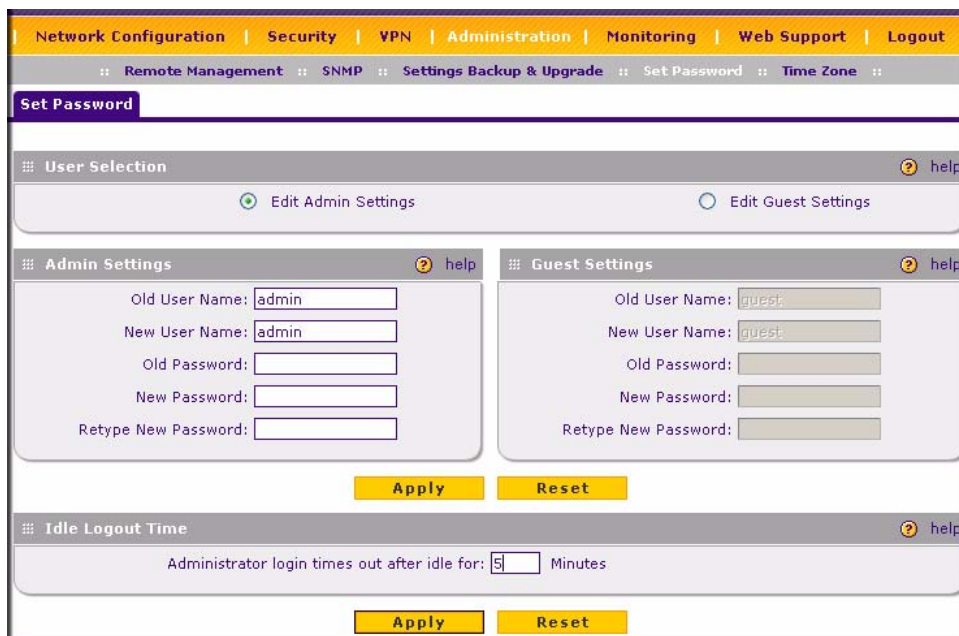



Figure 6-1

 **Note:** The password and time-out value you enter will be changed back to **password** and **5** minutes, respectively, after a factory defaults reset.

Enabling Remote Management Access

Using the Remote Management page, you can allow an administrator on the Internet to configure, upgrade, and check the status of your VPN firewall. You must be logged in locally to enable remote management (see [“Logging into the VPN Firewall”](#) on page 2-1).



Note: Be sure to change the default configuration password of the firewall to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters. See [“Changing Passwords and Settings”](#) on page 6-8 for the procedure on how to do this.

The screenshot shows the 'Remote Management' configuration page. At the top, there is a navigation bar with links: Network Configuration, Security, VPN, Administration, Monitoring, Web Support, and Logout. Below that is a breadcrumb trail: Remote Management :: SNMP :: Settings Backup & Upgrade :: Set Password :: Time Zone. The main content area is titled 'Remote Management' and contains the following options:

- Allow Remote Management?**
 - Yes
 - No
- Everyone (Be sure to change default password)
- IP address range:
 - From: [0].[0].[0].[0] To: [0].[0].[0].[0]
- Only this PC: [0].[0].[0].[0]
- Port Number: [8080]

At the bottom of the form are two buttons: 'Apply' and 'Reset'.

Figure 6-2

To configure your firewall for Remote Management:

1. Select **Administration** from the main menu and **Remote Management** from the submenu. The **Remote Management** screen will display.
2. Check **Allow Remote Management** radio box.
3. Specify what external addresses will be allowed to access the firewall’s remote management.



Note: For enhanced security, restrict access to as few external IP addresses as practical.

- a. To allow access from any IP address on the Internet, select Everyone.

The SNMP Configuration table lists the SNMP configurations by:

- **IP Address:** The IP address of the SNMP manager.
- **Port:** The trap port of the configuration.
- **Community:** The trap community string of the configuration.

To create a new SNMP configuration entry:

1. Select **Administration** from the main menu and **SNMP** from the submenu. The **SNMP** screen will display.
2. Under **Create New SNMP Configuration Entry**, enter the IP Address of the SNMP manager in the **IP Address** field and the Subnet Mask in the **Subnet Mask** field.
 - If you want to allow only the host address to access the VPN firewall and receive traps (for example, see [Figure 6-3](#)), enter an IP Address of, for example, 192.168.1.100 with a Subnet Mask of 255.255.255.**255**.
 - If you want to allow a subnet access to the VPN firewall through SNMP, enter an IP address of, for example, 192.168.1.100 with a Subnet Mask of 255.255.255.**0**. The traps will still be received on 192.168.1.100, but the entire subnet will have access through the community string.
 - If you want to make the VPN firewall globally accessible using the community string, but still receive traps on the host, enter 0.0.0.0 as the Subnet Mask and an IP Address for where the traps will be received.
3. Enter the trap port number of the configuration in the **Port** field. The default is 162.
4. Enter the trap community string of the configuration in the **Community** field.
5. Click **Add** to create the new configuration. The entry will display in the **SNMP Configuration** table.
6. Click **Edit** in the **Action** column adjacent to the entry to modify or change the selected configuration.

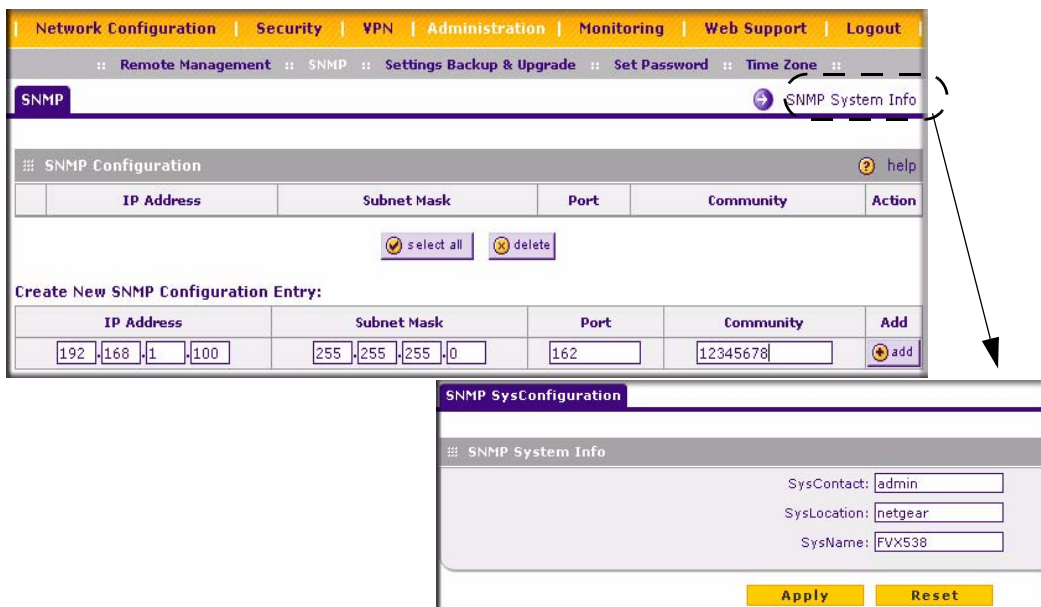


Figure 6-3

The **SNMP System Info** link displays the VPN firewall identification information available to the SNMP Manager: System Contact, System Location, and System name.

To modify the SNMP System contact information:

1. Click the **SNMP System Info** link. The **SNMP SysConfiguration** screen will display.
2. Modify any of the contact information that you want the SNMP Manager to use.
3. Click **Apply** to save your settings.

Settings Backup and Firmware Upgrade

Once you have installed the VPN firewall and have it working properly, you should back up a copy of your setting so that it is if something goes wrong. When you backup the settings, they are saved as a file on your computer. You can then restore the VPN firewall settings from this file. The **Settings Backup and Firmware Upgrade** screen allows you to:

- Back up and save a copy of your current settings
- Restore saved settings from the backed-up file.
- Revert to the factory default settings.

- Upgrade the VPN firewall firmware from a saved file on your hard disk to use a different firmware version.

Backup and Restore Settings

To backup and restore settings:

1. Select **Administration** from the main menu and **Settings Backup & Upgrade** from the submenu. The **Settings Backup and Firmware Upgrade** screen will display.
2. Click **backup** to save a copy of your current settings.

If your browser isn't set up to save downloaded files automatically, locate where you want to save the file, specify file name, and click Save. If you have your browser set up to save downloaded files automatically, the file will be saved to your browser's download location on the hard disk.



Warning: Once you start restoring settings or erasing the router, do NOT interrupt the process. Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until it finishes restarting!

To restore settings from a backup file:

1. Click **Browse**. Locate and select the previously saved backup file (by default, netgear.cfg).
2. When you have located the file, click **restore**.

An Alert page will appear indicating the status of the restore operation. You must manually restart the VPN firewall for the restored settings to take effect.

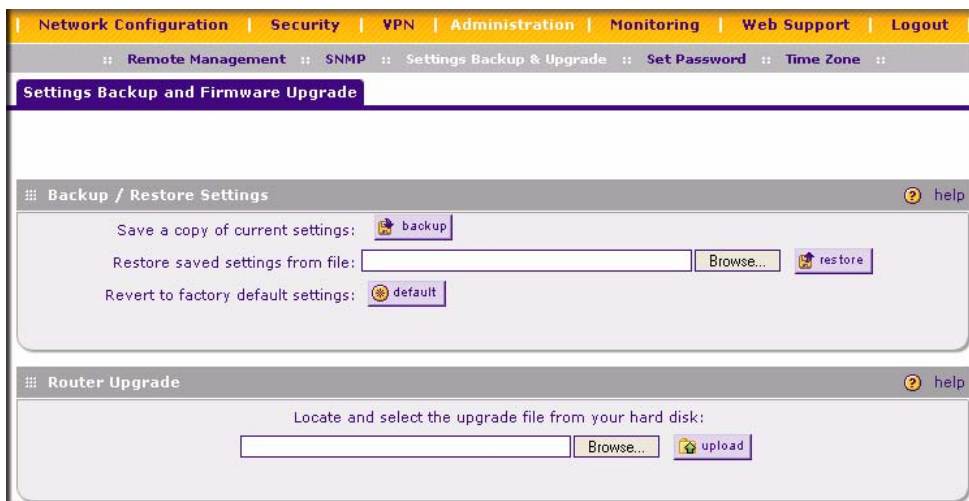
To reset the router to the original factory default settings:

Click **default**

You must manually restart the VPN firewall in order for the default settings to take effect. After rebooting, the router's password will be **password** and the LAN IP address will be **192.168.1.1**. The VPN firewall will act as a DHCP server on the LAN and act as a DHCP client to the Internet.



Warning: When you click **default**, your router settings will be erased. All firewall rules, VPN policies, LAN/WAN settings and other settings will be lost. Please backup your settings if you intend on using them!

**Figure 6-4**

Router Upgrade

You can install a different version of the VPN firewall firmware from the **Settings Backup and Firmware Upgrade** screen. To view the current version of the firmware that your VPN firewall is running, select **Monitoring** from the main menu. The **Router Status** screen on the will display all of the VPN firewall router statistics. When you upgrade your firmware, the Firmware Version will change to reflect the new version.

To download a firmware version:

1. Go to the NETGEAR Web site at <http://www.netgear.com/support> and click on **Downloads**.
2. From the **Product Selection** pull-down menu, select your product. Select the software version and follow the **To Install** steps to download your software.

After downloading an upgrade file, you may need to unzip (uncompress) it before upgrading the router. If Release Notes are included in the download, read them before continuing.



Warning: Once you click **Upload** do NOT interrupt the router!

To upgrade router software:

1. Select **Administration** from the main menu and **Settings Backup and Firmware Upgrade** from the submenu. The **Settings Backup and Firmware Upgrade** screen will display.
2. Click **Browse** in the **Router Upgrade** section.
3. Locate the downloaded file and click **Upload**. This will start the software upgrade to your VPN firewall router. This may take some time. At the conclusion of the upgrade, your router will reboot.



Warning: Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until the router finishes the upgrade! When the Test light turns off, wait a few more seconds before doing anything.

4. After the VPN firewall has rebooted, select **Monitoring** and confirm the new firmware version to verify that your router now has the new software installed.



Note: In some cases, such as a major upgrade, it may be necessary to erase the configuration and manually reconfigure your router after upgrading it. Refer to the Release Notes included with the software to find out if this is required.

Setting the Time Zone

Date, time and NTP Server designations can be input on the **Time Zone** screen. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers. Select **Administration** from the main menu and **Time Zone** from the submenu. The **Time Zone** screen will display.

To set Time, Date and NTP servers:

1. From the **Date/Time** pull-down menu, select the Local Time Zone. This is required in order for scheduling to work correctly. The VPN firewall includes a Real-Time Clock (RTC), which it uses for scheduling.
2. If supported in your region, check the **Automatically Adjust for Daylight Savings Time** radio box.
3. Select a NTP Server option by checking one of the following radio boxes:
 - **Use Default NTP Servers:** If this is enabled, then the RTC (Real-Time Clock) is updated regularly by contacting a Default Netgear NTP Server on the Internet.

- **Use Custom NTP Servers:** If you prefer to use a particular NTP server, enable this instead and enter the name or IP address of an NTP Server in the **Server 1 Name/IP Address** field.

If required, you can also enter the address of another NTP server in the **Server 2 Name/IP Address** field. If you select this option and leave either the Server 1 or Server 2 fields empty, they will be set to the Default Netgear NTP servers.

4. Click **Apply** to save your settings or click **Cancel** to revert to your previous settings.



Figure 6-5

Monitoring the Router

You can be alerted to important events such as WAN port rollover, WAN traffic limits reached, and login failures and attacks. You can also view status information about the firewall, WAN ports, LAN ports, and VPN tunnels and program SNMP connections.

Enabling the Traffic Meter

To monitor traffic limits on each of the WAN ports, select **Administration** from the main menu and **Traffic Meter** from the submenu. The **Wan1 Traffic Meter** screen will display. (The WAN1 and WAN2 ports are programmed separately.) A WAN port shuts down once its traffic limit is reached if the **Block all traffic** feature is enabled.

The **Traffic Meter** screen also provides the following information:

- **Internet Traffic Statistics** – Displays statistics on Internet Traffic via the WAN port. If you have not enabled the Traffic Meter, these statistics are not available.
- **Traffic by Protocol** – Click this button to display Internet Traffic details. The volume of traffic for each protocol will be displayed in a sub-window. Traffic counters are updated in MBytes scale and the counter starts only when traffic passed is at least 1 MB.

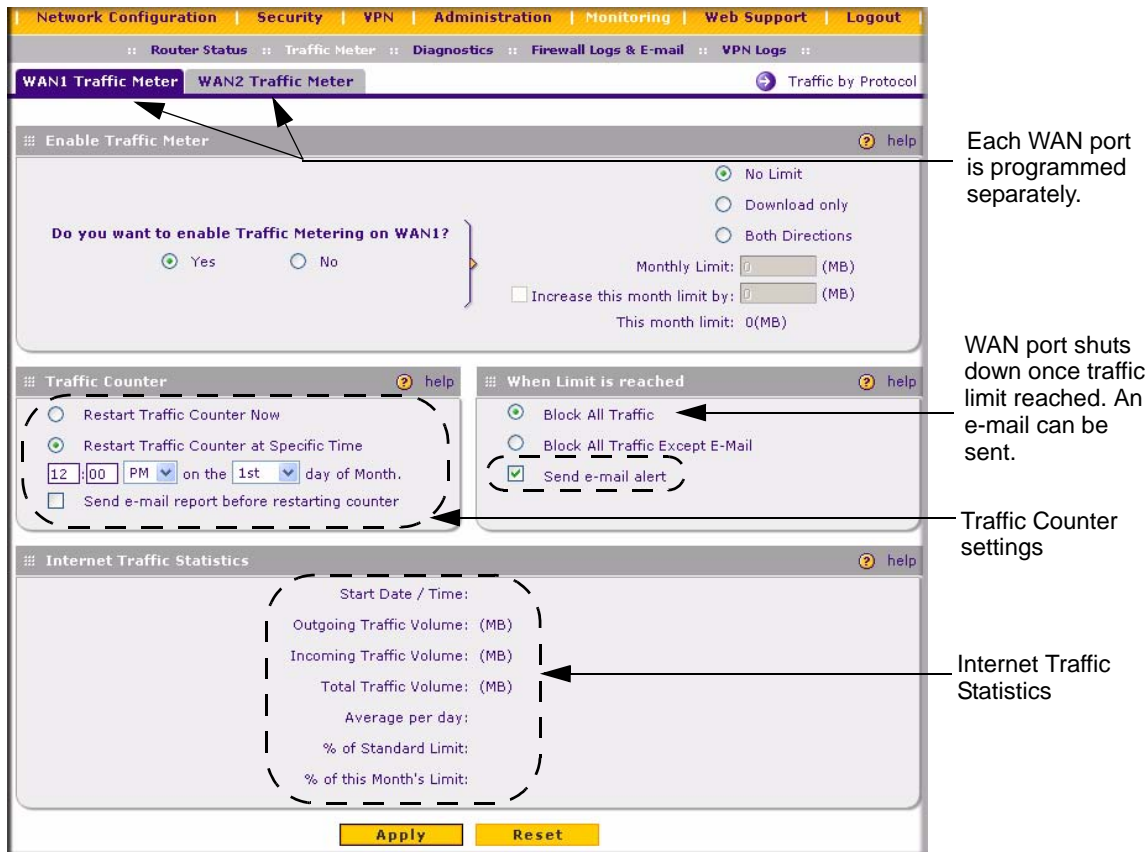


Figure 6-6

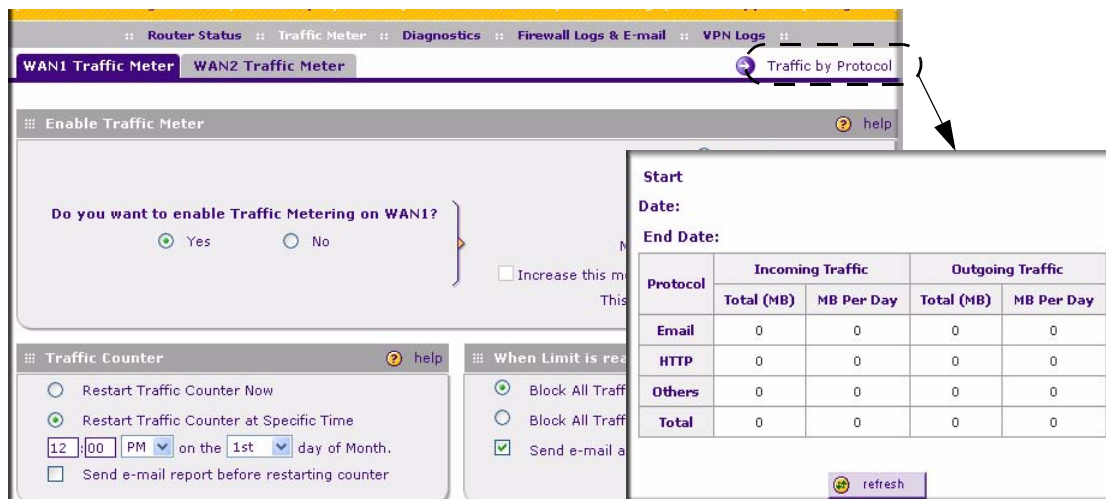


Figure 6-7

Setting Login Failures and Attacks Notification

Figure 6-8 shows the **Firewall Logs & E-mail** screen that is invoked by selecting **Monitoring** from the main menu and selecting **Firewall Logs & E-mail** from the submenu.

You can send a System log of firewall activities to an email address or a log of the firewall activities can be viewed, saved to a Syslog server, and then sent to an e-mail address. You can view the logs by clicking **View Logs**.

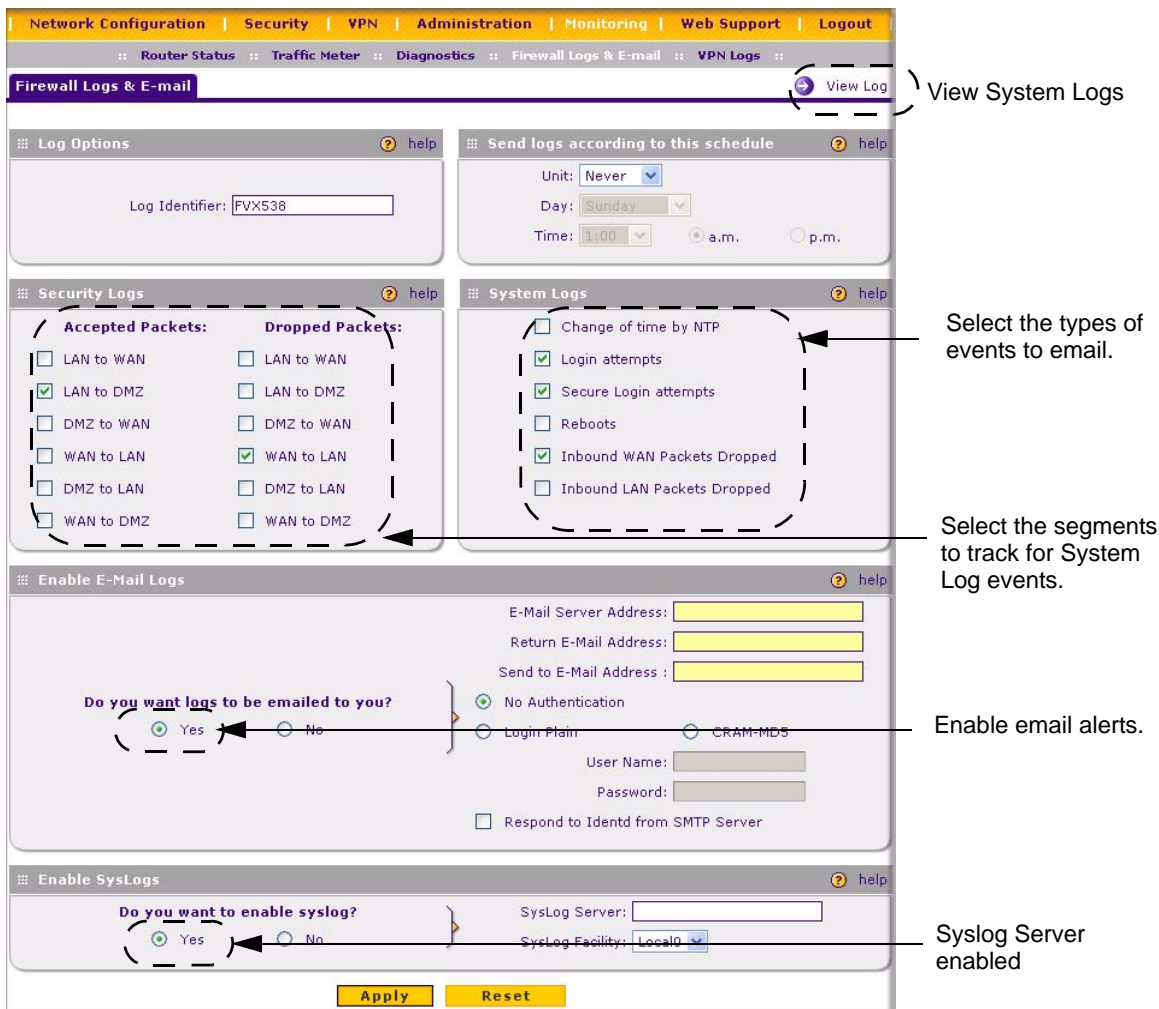


Figure 6-8

Monitoring Attached Devices

The **Groups and Hosts** menu contains a table of all IP devices that the VPN firewall has discovered on the local network. Select **Network Configuration** from the main menu and **LAN Groups** from the submenu. The **Groups and Hosts** screen will display.



Figure 6-9

The network database is an automatically-maintained list of all known PCs and network devices. PCs and devices become known by the following methods:

- **DHCP Client Requests** – By default, the DHCP server in this Router is enabled, and will accept and respond to DHCP client requests from PCs and other network devices. These requests also generate an entry in the network database. Because of this, leaving the DHCP Server feature enabled (on the LAN Setup screen) is strongly recommended.
- **Scanning the Network** – The local network is scanned using standard methods such as ARP. This will detect active devices which are not DHCP clients. However, sometimes the name of the PC or device cannot be accurately determined and will be shown as Unknown.


The **Known PCs and Devices** table lists all current entries in the network database. For each PC or device, the following data is displayed.

Table 6-1. Known PCs and Devices

Item	Description
Name	The name of the PC or device. Sometimes, this can not be determined, and will be listed as Unknown. In this case, you can edit the entry to add a meaningful name.
IP Address	The current IP address. For DHCP clients, where the IP address is allocated by the DHCP Server in this device, this IP address will not change. Where the IP address is set on the PC (as a fixed IP address), you may need to update this entry manually if the IP address on the PC is changed.

Table 6-1. Known PCs and Devices (continued)

Item	Description
MAC Address	The MAC address of the PC. The MAC address is a low-level network identifier which is fixed at manufacture.
Group	Each PC or device must be in a single group. The Group column indicates which group each entry is in. By default, all entries are in the Group1.



Note: If the VPN firewall is rebooted, the table data is lost until the VPN firewall rediscovers the devices.

Viewing Port Triggering Status

You can view the status of Port Triggering by selecting **Security** from the main menu and **Port Triggering** from the submenu. When the **Port Triggering** screen display, click the **Status** link.

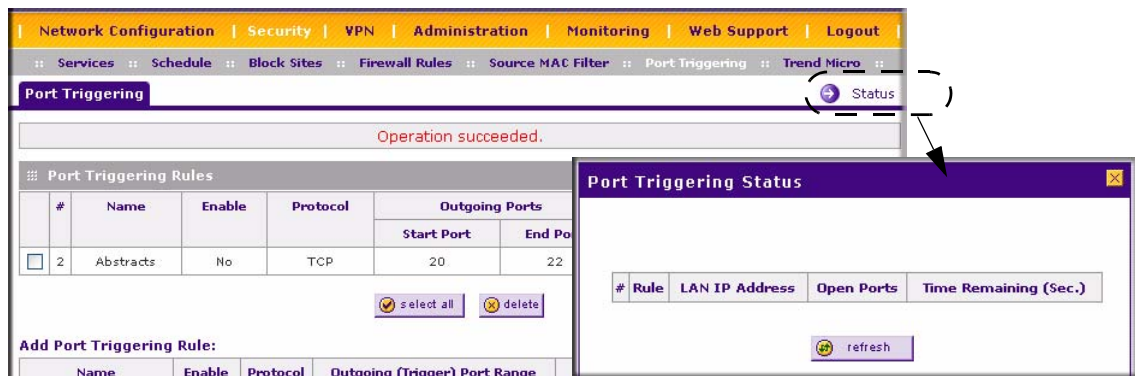


Figure 6-10

Table 6-2. Port Triggering Status data

Item	Description
Rule	The name of the Rule.
LAN IP Address	The IP address of the PC currently using this rule.
Open Ports	The Incoming ports which are associated the this rule. Incoming traffic using one of these ports will be sent to the IP address above.
Time Remaining	The time remaining before this rule is released, and thus available for other PCs. This timer is restarted whenever incoming or outgoing traffic is received.

Viewing Router Configuration and System Status

The **Router Status** screen provides status and usage information. Select **Monitoring** from the main menu and **Router Status** from the submenu. The **Router Status** screen will display.

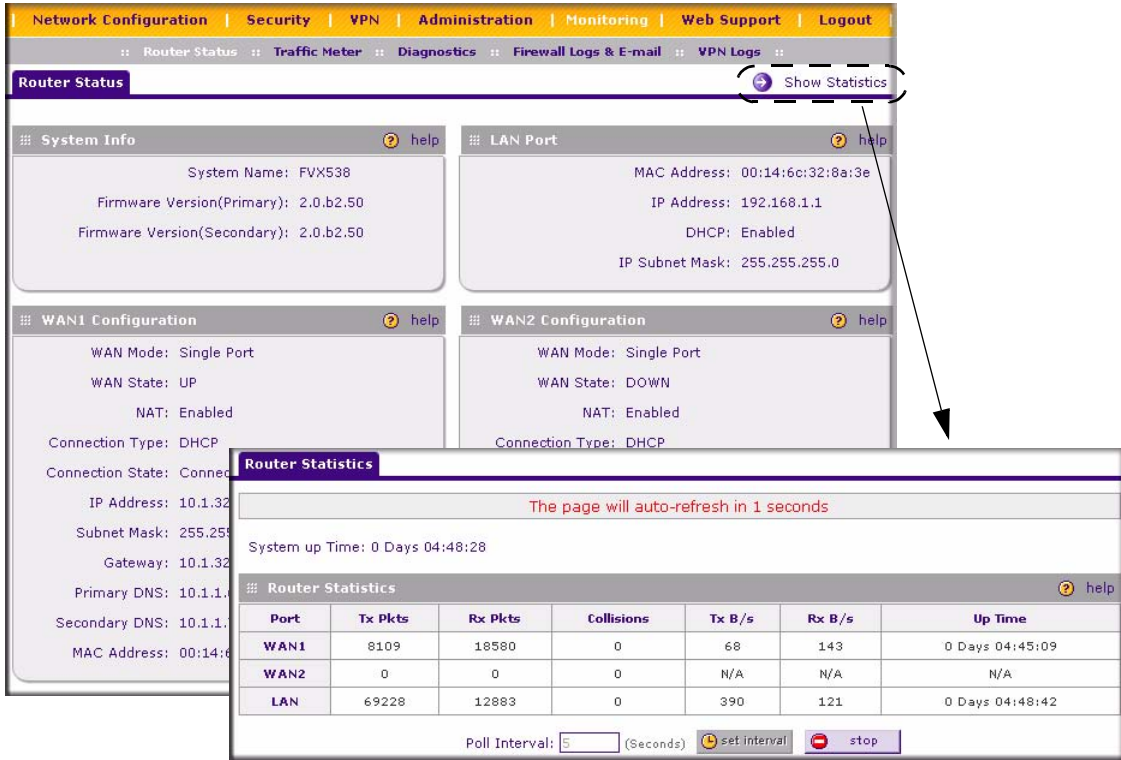


Figure 6-11

Table 6-3. Router Status Fields

Item	Description
System Name	This is the Account Name that you entered in the Basic Settings page.
Firmware Version	This is the current software the router is using. This will change if you upgrade your router.
LAN Port	Displays the current settings for MAC address, IP address, DHCP role and IP Subnet Mask that you set in the LAN IP Setup page. DHCP can be either Server or None.

Table 6-3. Router Status Fields

Item	Description
WAN1 Configuration	Indicates whether the WAN Mode is Single, Dual, or Rollover, and whether the WAN State is UP or DOWN. It also displays if: <ul style="list-style-type: none"> • NAT is Enabled or Disabled. • Connection Type: DHCP enabled or disabled. • Connection State • WAN IP Address • Subnet Mask • Gateway Address • Primary and Secondary DNS Server Addresses • MAC Address.
WAN2 Configuration	Displays the same details as for WAN1 Configuration.



Note: The **Router Status** screen displays current settings and statistics for your router. As this information is read-only, any changes must be made on other pages.

Monitoring WAN Ports Status

You can monitor the status of both of the WAN connections, the Dynamic DNS Server connections, and the DHCP Server connections. Select **Network Configuration** from the main menu and **WAN Settings** from the submenu. The **WAN1 ISP Settings** screen will display. Click the **WAN Status** link to obtain status on the WAN1 port. Select the **WAN2 IAP Settings** tab and click the **WAN Status** link to obtain status on the WAN2 port

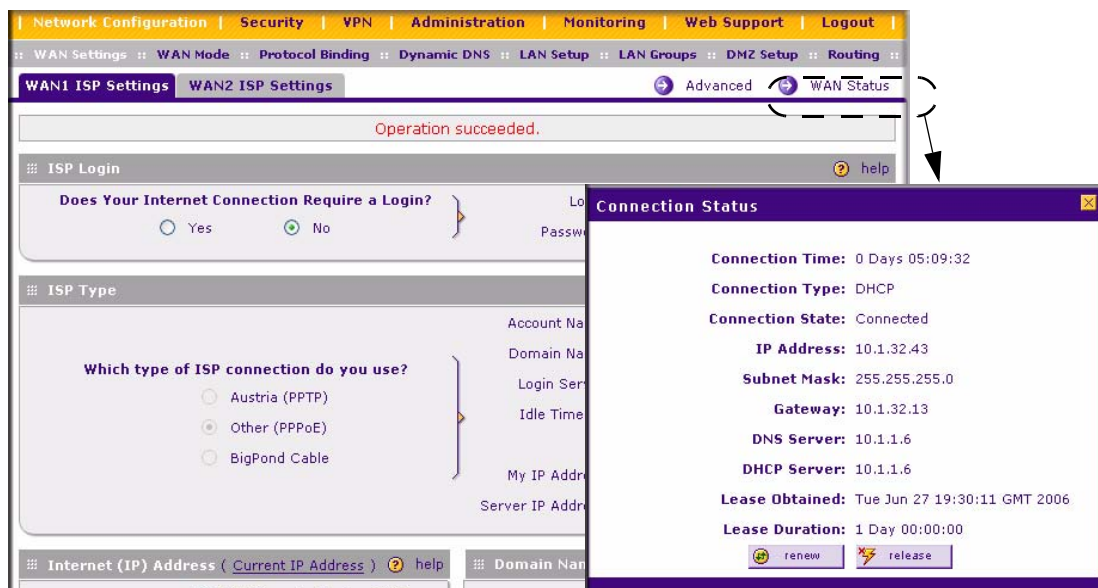


Figure 6-12

Monitoring VPN Tunnel Connection Status

You can view the status of the VPN tunnels by selecting **VPN** from the main menu and **Connection Status** from the submenu. The **IPSec Connection Status** screen will display.



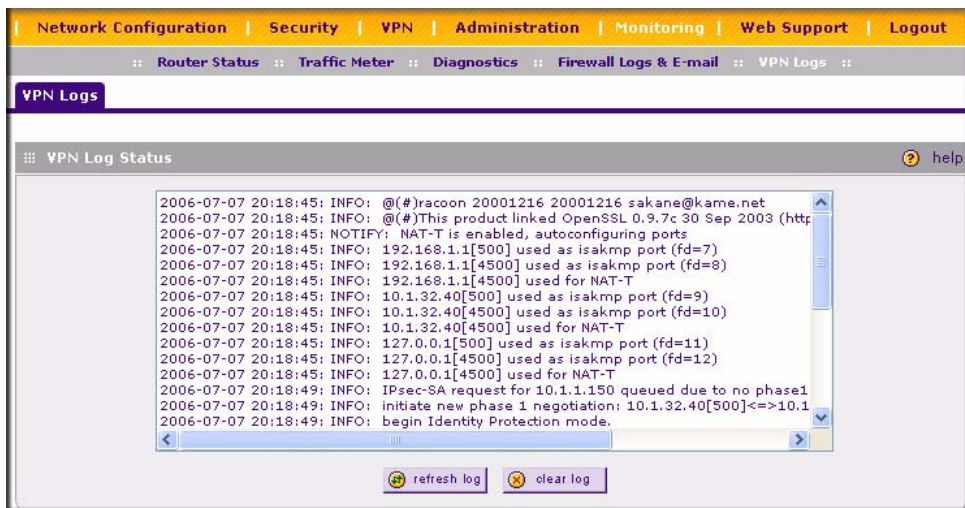
Figure 6-13

Table 6-4. VPN Status data

Item	Description
Policy Name	The name of the VPN policy associated with this SA.
Endpoint	The IP address on the remote VPN Endpoint.
Tx (KB)	The amount of data transmitted over this SA.
Tx (Packets)	The number of IP packets transmitted over this SA.
State	The current status of the SA.Phase 1 is Authentication phase and Phase 2 is Key Exchange phase.
Action	Use this button to terminate/build the SA (connection) if required.

VPN Logs

The **VPN Logs** screen gives log details for recent VPN activity. Select **Monitoring** from the main menu and **VPN Logs** from the submenu to view the VPN Logs. You can refresh the log display to view the most recent entries, or clear the log display to delete all the log entries.

**Figure 6-14**

DHCP Log

You can view the DHCP log from the **LAN Setup** screen. Select **Network Configuration** from the main menu and **LAN Setup** from the submenu. When the **LAN Setup** screen displays, click the **DHCP Log** link.

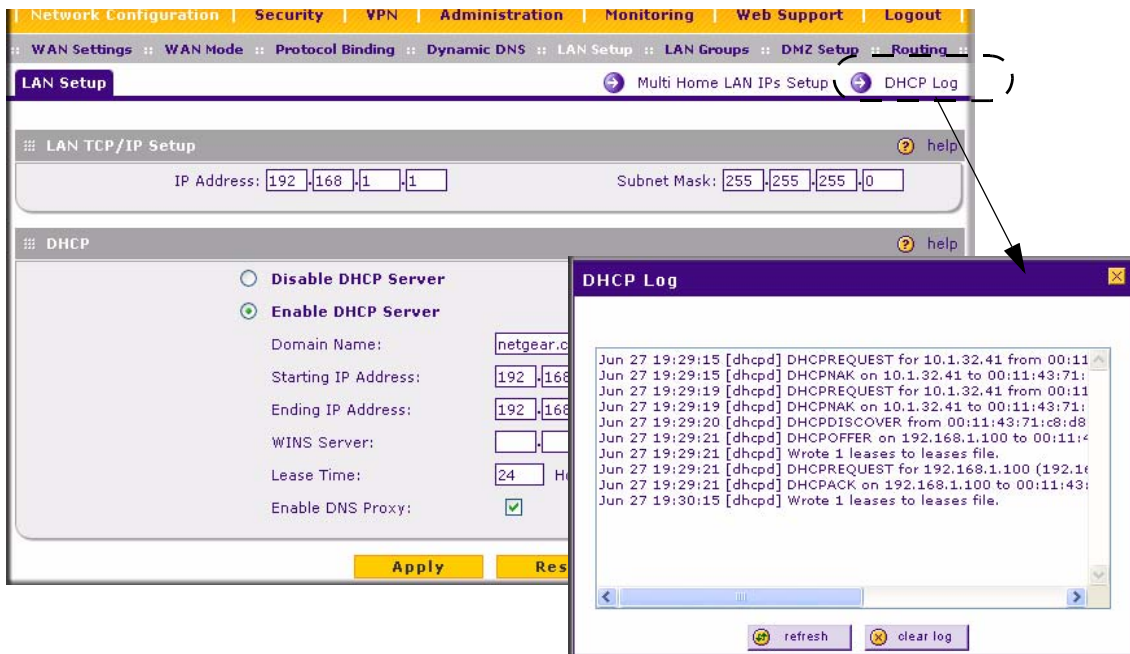


Figure 6-15

Performing Diagnostics

You can perform diagnostics such as pinging an IP address, performing a DNS lookup, displaying the routing table, rebooting the firewall, and capturing packets. Select **Monitoring** from the main menu and **Diagnostics** from the submenu. The **Diagnostics** screen will display.



Note: For normal operation, diagnostics are not required.

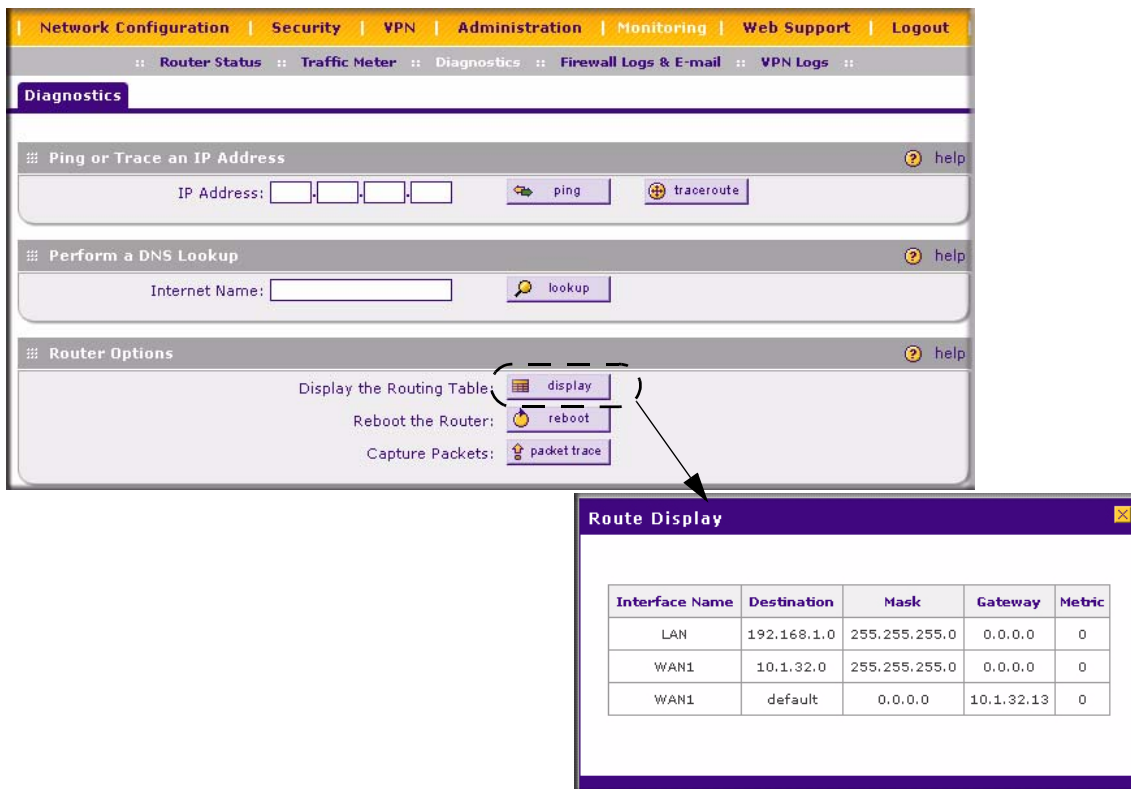


Figure 6-16

Table 6-5. Diagnostics

Item	Description
Ping or Trace an IP address	Ping – Used to send a ping packet request to a specified IP address—most often, to test a connection. If the request times out (no reply is received), it usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping. The ping results will be displayed in a new screen; click “Back” on the Windows menu bar to return to the Diagnostics screen.
	Traceroute (often called Trace Route) – Lists all Routers between the source (this device) and the destination IP address. The Trace Route results will be displayed in a new screen; click “Back” on the Windows menu bar to return to the Diagnostics screen.
Perform a DNS Lookup	A DNS (Domain Name Server) converts the Internet name (e.g. www.netgear.com) to an IP address. If you need the IP address of a Web, FTP, Mail or other Server on the Internet, you can do a DNS lookup to find the IP address.

Table 6-5. Diagnostics (continued)

Item	Description
Display the Routing Table	This operation will display the internal routing table. This information is used, most often, by Technical Support.
Reboot the Router	Used to perform a remote reboot (restart). You can use this if the Router seems to have become unstable or is not operating normally. Note: Rebooting will break any existing connections either to the Router (such as this one) or through the Router (for example, LAN users accessing the Internet). However, connections to the Internet will automatically be re-established when possible.
Packet Trace	Packet Trace selects the interface and starts the packet capture on that interface.

Chapter 7

Troubleshooting

This chapter provides troubleshooting tips and information for your ProSafe VPN Firewall 200. After each problem description, instructions are provided to help you diagnose and solve the problem.

Basic Functions

After you turn on power to the firewall, the following sequence of events should occur:

1. When power is first applied, verify that the PWR LED is on.
2. After approximately 2 minutes, verify that:
 - a. The TEST LED is not lit.
 - b. The LAN port LEDs are lit for any local ports that are connected.
 - c. The Internet port LED is lit.

If a port's LED is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED will be amber.

If any of these conditions does not occur, refer to the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your firewall is turned on:

- Make sure that the power cord is properly connected to your firewall and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact technical support.

LEDs Never Turn Off

When the firewall is turned on, the LEDs turn on for about 10 seconds and then turn off. If all the LEDs stay on, there is a fault within the firewall.

If all LEDs are still on one minute after power up:

- Cycle the power to see if the firewall recovers.
- Clear the firewall's configuration to factory defaults. This will set the firewall's IP address to 192.168.1.1. This procedure is explained in [“Restoring the Default Configuration and Password” on page 7-7](#).

If the error persists, you might have a hardware problem and should contact technical support.

LAN or Internet Port LEDs Not On

If either the LAN LEDs or Internet LED do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the firewall and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:

When connecting the firewall's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Troubleshooting the Web Configuration Interface

If you are unable to access the firewall's Web Configuration interface from a PC on your local network, check the following:

- Check the Ethernet connection between the PC and the firewall as described in the previous section.

- Make sure your PC's IP address is on the same subnet as the firewall. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.0.2 to 192.168.0.254.



Note: If your PC's IP address is shown as 169.254.x.x: Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the firewall and reboot your PC.

- If your firewall's IP address has been changed and you don't know the current IP address, clear the firewall's configuration to factory defaults. This will set the firewall's IP address to 192.168.1.1. This procedure is explained in [“Restoring the Default Configuration and Password” on page 7-7](#).



Tip: If you don't want to revert to the factory default settings and lose your configuration settings, you can reboot the router and use sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the router's LAN interface address.

- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the firewall does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the APPLY button before moving to another menu or tab, or your changes are lost.
- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

If your firewall is unable to access the Internet, you should first determine whether the firewall is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your firewall must request an IP address from the ISP. You can determine whether the request was successful using the Web Configuration Manager.

To check the WAN IP address:

1. Launch your browser and select an external site such as www.netgear.com
2. Access the Main Menu of the firewall's configuration at <http://192.168.1.1>
3. Under the Monitoring menu, select Router Status
4. Check that an IP address is shown for the WAN Port
If 0.0.0.0 is shown, your firewall has not obtained an IP address from your ISP.

If your firewall is unable to obtain an IP address from the ISP, you may need to force your cable or DSL modem to recognize your new firewall by performing the following procedure:

1. Turn off power to the cable or DSL modem.
2. Turn off power to your firewall.
3. Wait five minutes and reapply power to the cable or DSL modem.
4. When the modem's LEDs indicate that it has reacquired sync with the ISP, reapply power to your firewall.

If your firewall is still unable to obtain an IP address from the ISP, the problem may be one of the following:

- Your ISP may require a login program.
Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, you may have incorrectly set the login name and password.
- Your ISP may check for your PC's host name.
Assign the PC Host Name of your ISP account as the Account Name in the Basic Settings menu.
- Your ISP only allows one Ethernet MAC address to connect to the Internet, and may check for your PC's MAC address. In this case:
 - Inform your ISP that you have bought a new network device, and ask them to use the firewall's MAC address; or

- Configure your firewall to spoof your PC's MAC address. This can be done in the Basic Settings menu. Refer to [“Manually Configuring Your Internet Connection”](#) on page 2-5.

If your firewall can obtain an IP address, but your PC is unable to load any Web pages from the Internet:

- Your PC may not recognize any DNS server addresses.
A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. You may configure your PC manually with DNS addresses, as explained in your operating system documentation.
- Your PC may not have the firewall configured as its TCP/IP gateway.

Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and firewalls contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the Ping utility in your PC or workstation.

Testing the LAN Path to Your Firewall

You can ping the firewall from your PC to verify that the LAN path to your firewall is set up correctly.

To ping the firewall from a PC running Windows 95 or later:

1. From the Windows toolbar, click **Start** and select **Run**.
2. In the field provided, type “ping” followed by the IP address of the firewall; for example:

```
ping 192.168.1.1
```

3. Click **OK**. A message, similar to the following, should display:

```
Pinging <IP address> with 32 bytes of data
```

If the path is working, you will see this message:

```
Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you will see this message:

```
Request timed out
```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
 - Make sure the LAN port LED is on. If the LED is off, follow the instructions in [“LAN or Internet Port LEDs Not On”](#) on page 7-2.
 - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and firewall.
- Wrong network configuration
 - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
 - Verify that the IP address for your firewall and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

```
PING -n 10 <IP address>
```

where *<IP address>* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your firewall listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel.
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your firewall to “clone” or “spoof” the MAC address from the authorized PC. Refer to [“Manually Configuring Your Internet Connection”](#) on page 2-5.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the firewall's administration password to **password** and the IP address to 192.168.1.1. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the firewall (see [“Backup and Restore Settings” on page 6-14](#)).
- Use the reset button on the rear panel of the firewall. Use this method for cases when the administration password or IP address is not known.

To restore the factory default configuration settings without knowing the administration password or IP address, you must use the reset button on the rear panel of the firewall.

To restore the factory defaults:

1. Press and hold the reset button until the Test LED turns on and begins to blink (about 10 seconds).
2. Release the reset button and wait for the firewall to reboot.

Problems with Date and Time

The E-Mail menu in the Content Filtering section displays the current date and time of day. The VPN firewall uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The firewall has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the firewall, wait at least five minutes and check the date and time again.
- Time is off by one hour. Cause: The firewall does not automatically sense Daylight Savings Time. Check the Time Zone menu, and check or uncheck the box marked “Adjust for Daylight Savings Time”.

Appendix A

Default Settings and Technical Specifications

You can use the reset button located on the front of your device to reset all settings to their factory defaults. This is called a hard reset.

- To perform a hard reset, push and hold the reset button for approximately 5 seconds (until the TEST LED blinks rapidly). Your device will return to the factory configuration settings shown in [Table A-1](#) below.
- Pressing the reset button for a shorter period of time will simply cause your device to reboot.

Table A-1. VPN firewall Default Configuration Settings

Feature	Default Behavior
Router Login	
User Login URL	http://192.168.1.1
User Name (case sensitive)	admin
Login Password (case sensitive)	password
Internet Connection	
WAN MAC Address	Use Default address
WAN MTU Size	1500
Port Speed	AutoSense
Local Network (LAN)	
Lan IP	192.168.1.1
Subnet Mask	255.255.255.0
RIP Direction	None
RIP Version	Disabled
RIP Authentication	Disabled
DHCP Server	Enabled
DHCP Starting IP Address	192.168.1.2
DHCP Ending IP Address	192.168.1.100
DMZ	Disabled

Table A-1. VPN firewall Default Configuration Settings (continued)

Feature		Default Behavior
	Time Zone	GMT
	Time Zone Adjusted for Daylight Saving Time	Disabled
	SNMP	Disabled
	Remote Management	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the http port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
	Stealth Mode	Enabled

Technical specifications for the ProSafe VPN Firewall 200 are listed in the following table.

Table A-2. VPN firewall Technical Specifications

Feature		Specifications
Network Protocol and Standards Compatibility		
	Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
Power Adapter		
	North America:	120V, 60 Hz, input
	United Kingdom, Australia:	240V, 50 Hz, input
	Europe:	230V, 50 Hz, input
	Japan:	100V, 50/60 Hz, input
Physical Specifications		
	Dimensions:	1.7 x 13 x 8.2 in.
	Weight:	2 kg (4.5 lb)

Table A-2. VPN firewall Technical Specifications (continued)

Feature	Specifications
Environmental Specifications	
Operating temperature:	0° to 40° C (32° to 104° F)
Operating humidity:	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	
Meets requirements of:	FCC Part 15 Class B
	VCCI Class B
	EN 55 022 (CISPR 22), Class B
Interface Specifications	
LAN:	10BASE-T or 100BASE-Tx, RJ-45
WAN:	10BASE-T or 100BASE-Tx; 1000BASE-T

Appendix B

Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing:	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Communications:	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing a Computer for Network Access:	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking (VPN):	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary	http://documentation.netgear.com/reference/enu/glossary/index.htm

Appendix C

Network Planning for Dual WAN Ports

This appendix describes the factors to consider when planning a network using a firewall that has dual WAN ports.

What You Will Need to Do Before You Begin

The ProSafe VPN Firewall 200 is a powerful and versatile solution for your networking needs. But to make the configuration process easier and to understand all of the choices available to you, you need to think through the following items before you begin:

1. Plan your network
 - a. Determine whether you are going to use one or both WAN ports. For one WAN port, you may need a fully qualified domain name either for convenience or if you have a dynamic IP address.
 - b. If you are going to use both WAN ports, determine whether you are going to use them in rollover mode for increased system reliability or load balancing mode for maximum bandwidth efficiency. See the topics in this appendix for more information. Your decision has the following implications:
 - Fully qualified domain name
 - For rollover mode, you are going to need a fully qualified domain name to implement features such as exposed hosts and virtual private networks.
 - For load balancing mode, you may still need a fully qualified domain name either for convenience or if you have a dynamic IP address.
 - Protocol binding
 - For rollover mode, protocol binding does not apply.
 - For load balancing mode, you need to decide which protocols you want to bind to a specific WAN port if you are going to take advantage of this option (you will make these selections in [“Configuring the WAN Mode \(Required for Dual WAN\)”](#) on [page 2-10](#)).

- You can also add your own service protocols to the list (see [“Services-Based Rules”](#) on page 4-2 for information on how to do this).
3. Set up your accounts
 - a. Have active Internet services such as that provided by cable or DSL broadband accounts and locate the Internet Service Provider (ISP) configuration information.
 - In this document, the WAN side of the network is presumed to be provisioned as shown in [Figure C-1](#) with two ISPs connected to the VPN firewall through separate physical facilities.
 - Each FVX538 WAN port must be configured separately, however, whether you are using a separate ISP for each WAN port or are having the traffic of both WAN ports routed through the same ISP. You will need your ISP information for [“Configuring the Internet Connections to Your ISPs”](#) on page 2-2.

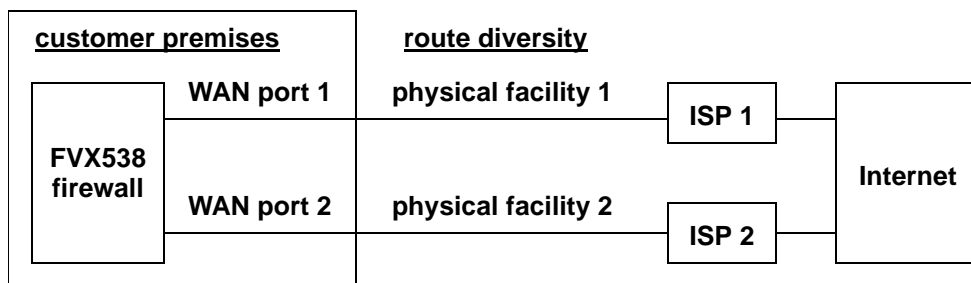


Figure C-1

- If your ISPs charge by the amount of bandwidth you use each month, you may want to consider setting up a traffic meter to keep track of your traffic (see [“To manually configure your WAN1 ISP Settings:”](#) on page 2-5 if you want to do this).
- b. Contact a Dynamic DNS Service and set up your fully qualified domain names if you need or want them. You will need your fully qualified domain names for [“Configuring Dynamic DNS \(If Needed\)”](#) on page 2-15.
3. Plan your network management approach
 - The VPN firewall is capable of being managed remotely, but this feature must be enabled locally after each factory default reset.

You are strongly advised to change the default **password** password to something that is more secure at the time you enable remote management.

You make these selections during [“Logging into the VPN Firewall”](#) on page 2-1.

- There are a variety of WAN options you can choose when the factory default settings are not applicable to your installation. These include enabling a WAN port to respond to a ping and setting MTU size, port speed, and upload bandwidth. You will make these choices in “[Configuring the Advanced WAN Options \(If Needed\)](#)” on page 2-18.
4. Prepare to physically connect the firewall to cable or DSL modems and a computer. Instruction for connecting your VPN firewall are in *Installation Guide, FVX538 ProSafe VPN Firewall 200*.

Cabling and Computer Hardware Requirements

To use the VPN firewall on your network, each computer must have an installed Ethernet Network Interface Card (NIC) and an Ethernet cable. If the computer will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable such as the one provided with your firewall.

Computer Network Configuration Requirements

The FVX538 includes a built-in Web Configuration Manager. To access the configuration menus on the FVX538, you must use a Java-enabled Web browser program that supports HTTP uploads such as Microsoft Internet Explorer or Netscape Navigator. NETGEAR recommends using Internet Explorer or Netscape Navigator 4.0 or above. Free browser programs are readily available for Windows, Macintosh, or UNIX/Linux.

For the initial connection to the Internet and configuration of your firewall, you will need to connect a computer to the firewall that is set to automatically get its TCP/IP configuration from the firewall via DHCP.



Note: For help with DHCP configuration, please refer to the link in [Appendix B, “Related Documents.”](#)

The cable or DSL modem broadband access device must provide a standard 10 Mbps (10BASE-T) Ethernet interface.

Internet Configuration Requirements

Depending on how your ISPs set up your Internet accounts, you will need one or more of these configuration parameters to connect your firewall to the Internet:

- Host and Domain Names
- ISP Login Name and Password
- ISP Domain Name Server (DNS) Addresses

- Fixed IP Address which is also known as Static IP Address

Where Do I Get the Internet Configuration Parameters?

There are several ways you can gather the required Internet connection information.

- Your ISPs provide all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISPs to provide it or you can try one of the options below.
- If you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.
 - For Windows 95/98/ME, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
 - For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
 - For Macintosh computers, open the TCP/IP or Network control panel. Record all the settings for each section.
- You may also refer to the *FVX538 Resource CD* for the NETGEAR Router ISP Guide which provides Internet connection information for many ISPs.

Once you locate your Internet configuration parameters, you may want to record them on the page below.

Internet Connection Information Form

Print this page. Fill in the configuration parameters from your Internet Service Provider (ISP).

ISP Login Name: The login name and password are case sensitive and must be entered exactly as given by your ISP. For AOL customers, the login name is their primary screen name. Some ISPs use your full e-mail address as the login name. The Service Name is not required by all ISPs. If you connect using a login name and password, then fill in the following:

Login Name: _____ Password: _____

Service Name: _____

Fixed or Static IP Address: If you have a static IP address, record the following information. For example, 169.254.141.148 could be a valid IP address.

Fixed or Static Internet IP Address: _____

Gateway IP Address: _____

Subnet Mask: _____

ISP DNS Server Addresses: If you were given DNS server addresses, fill in the following:

Primary DNS Server IP Address: _____

Secondary DNS Server IP Address: _____

Host and Domain Names: Some ISPs use a specific host or domain name like **CCA7324-A** or **home**. If you haven't been given host or domain names, you can use the following examples as a guide:

- If your main e-mail account with your ISP is `aaa@yyy.com`, then use **aaa** as your host name. Your ISP might call this your account, user, host, computer, or system name.
- If your ISP's mail server is `mail.xxx.yyy.com`, then use **xxx.yyy.com** as the domain name.

ISP Host Name: _____ ISP Domain Name: _____

Fully Qualified Domain Name: Some organizations use a fully qualified domain name (FQDN) from a dynamic DNS service provider for their IP addresses.

Dynamic DSN Service Provider: _____ FQDN: _____

Overview of the Planning Process

The areas that require planning when using a firewall that has dual WAN ports include:

- Inbound traffic (e.g., port forwarding, port triggering, DMZ port)
- Virtual private networks (VPNs)

The two WAN ports can be configured on a mutually-exclusive basis to either:

- Rollover for increased reliability, or
- Balance the load for outgoing traffic.

These two categories of considerations interact to make the planning process more challenging.

Inbound Traffic

Unrequested incoming traffic can be directed to a PC on your LAN rather than being discarded. The mechanism for making the IP address public depends on whether the dual WAN ports are configured to either roll over or balance the loads. See [“Inbound Traffic” on page C-8](#) for further discussion.

Virtual Private Networks (VPNs)

A virtual private network (VPN) tunnel provides a secure communication channel between either two gateway VPN firewalls or between a remote PC client and gateway VPN firewall. As a result, the IP address of at least one of the tunnel end points must be known in advance in order for the other tunnel end point to establish (or re-establish) the VPN tunnel. See [“Virtual Private Networks \(VPNs\)” on page C-10](#) for further discussion.



Note: Once the gateway firewall WAN port rolls over, the VPN tunnel collapses and must be re-established using the new WAN IP address.

The Roll-over Case for Firewalls With Dual WAN Ports

Rollover (Figure C-2) for the dual WAN port case is different from the single gateway WAN port case when specifying the IP address. Only one WAN port is active at a time and when it rolls over, the IP address of the active WAN port always changes. Hence, the use of a fully-qualified domain name is always required, even when the IP address of each WAN port is fixed.

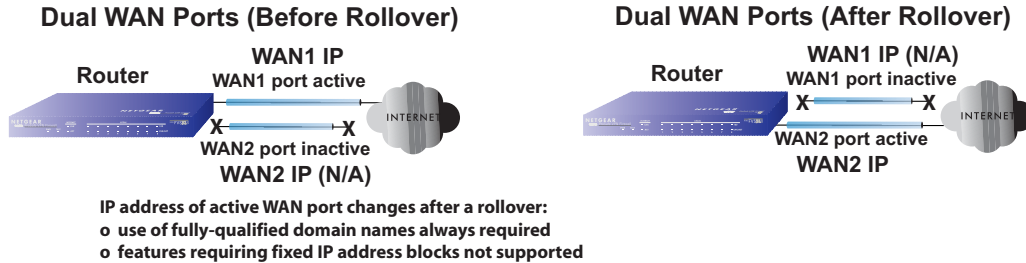


Figure C-2

Features such as multiple exposed hosts are not supported when using dual WAN port rollover because the IP addresses of each WAN port must be in the identical range of fixed addresses.

The Load Balancing Case for Firewalls With Dual WAN Ports

Load balancing (Figure C-3) for the dual WAN port case is similar to the single WAN port case when specifying the IP address. Each IP address is either fixed or dynamic based on the ISP: fully-qualified domain names must be used when the IP address is dynamic and are optional when the IP address is static.

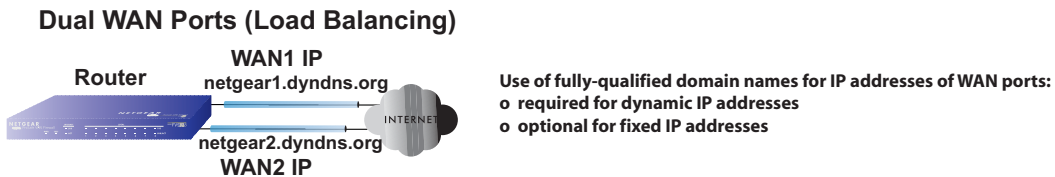


Figure C-3

Inbound Traffic

Incoming traffic from the Internet is normally discarded by the firewall unless the traffic is a response to one of your local computers or a service that you have configured in the Inbound Rules menu. Instead of discarding this traffic, you can have it forwarded to one or more LAN hosts on your network.

The addressing of the firewall's dual WAN port depends on the configuration being implemented:

Table C-1. IP addressing requirements for exposed hosts in dual WAN port systems

Configuration and WAN IP address		Single WAN Port (reference case)	Dual WAN Port Cases	
			Rollover	Load Balancing
Inbound traffic <ul style="list-style-type: none"> • Port forwarding • Port triggering • DMZ port 	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required

Inbound Traffic to Single WAN Port (Reference Case)

The Internet IP address of the firewall's WAN port must be known to the public so that the public can send incoming traffic to the exposed host when this feature is supported and enabled.

In the single WAN case (Figure C-4), the WAN's Internet address is either fixed IP or a fully-qualified domain name if the IP address is dynamic.



Figure C-4

Inbound Traffic to Dual WAN Port Systems

The IP address range of the firewall's WAN port must be both fixed and public so that the public can send incoming traffic to the multiple exposed hosts when this feature is supported and enabled.

Inbound Traffic: Dual WAN Ports for Improved Reliability

In the dual WAN port case with rollover (Figure C-5), the WAN's IP address will always change at rollover. A fully-qualified domain name must be used that toggles between the IP addresses of the WAN ports (i.e., WAN1 or WAN2).

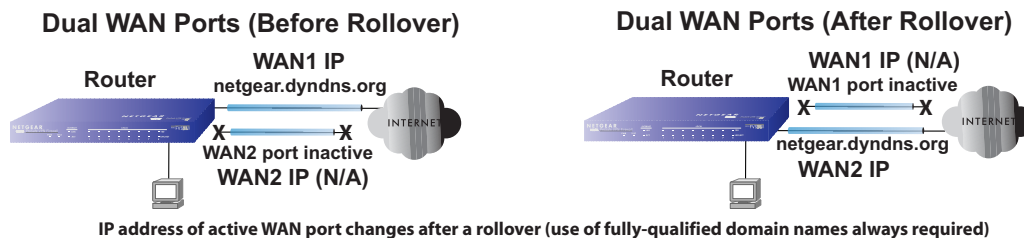


Figure C-5

Inbound Traffic: Dual WAN Ports for Load Balancing

In the dual WAN port case for load balancing (Figure C-6), the Internet address of each WAN port is either fixed if the IP address is fixed or a fully-qualified domain name if the IP address is dynamic.



Note: Load balancing is implemented for outgoing traffic and not for incoming traffic. Consider making one of the WAN port Internet addresses public and keeping the other one private in order to maintain better control of WAN port traffic.

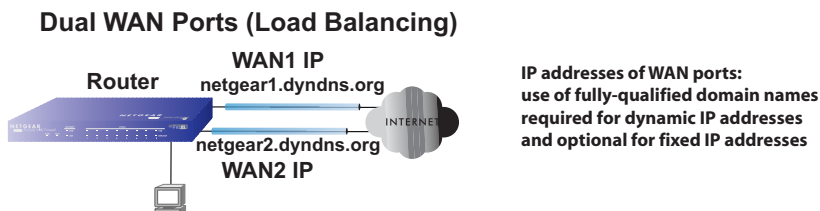


Figure C-6

Virtual Private Networks (VPNs)

When implementing virtual private network (VPN) tunnels, a mechanism must be used for determining the IP addresses of the tunnel end points. The addressing of the firewall's dual WAN port depends on the configuration being implemented:

Table C-2. IP addressing requirements for VPNs in dual WAN port systems

Configuration and WAN IP address		Single WAN Port (reference case)	Dual WAN Port Cases	
			Rollover ^a	Load Balancing
VPN Road Warrior (client-to-gateway)	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required
VPN Gateway-to-Gateway	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required
VPN Telecommuter (client-to-gateway through a NAT router)	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required

a. All tunnels must be re-established after a rollover using the new WAN IP address.

For the single gateway WAN port case, the mechanism is to use a fully-qualified domain name (FQDN) when the IP address is dynamic and to use either an FQDN or the IP address itself when the IP address is fixed. The situation is different when dual gateway WAN ports are used in a rollover-based system.

- Rollover Case for Dual Gateway WAN Ports

Rollover ([Figure C-7](#)) for the dual gateway WAN port case is different from the single gateway WAN port case when specifying the IP address of the VPN tunnel end point. Only one WAN port is active at a time and when it rolls over, the IP address of the active WAN port always changes. Hence, the use of a fully-qualified domain name is always required, even when the IP address of each WAN port is fixed.



Note: Once the gateway router WAN port rolls over, the VPN tunnel collapses and must be re-established using the new WAN IP address.

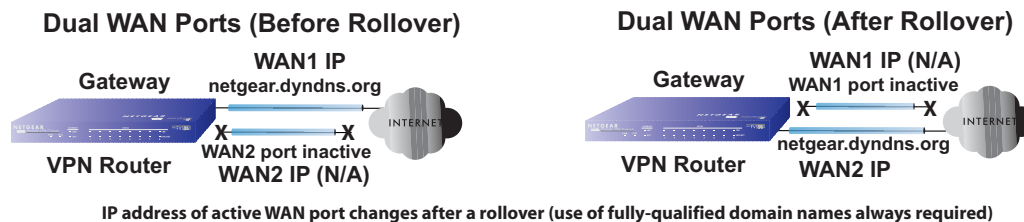


Figure C-7

- Load Balancing Case for Dual Gateway WAN Ports

Load balancing (Figure C-8) for the dual gateway WAN port case is the same as the single gateway WAN port case when specifying the IP address of the VPN tunnel endpoint. Each IP address is either fixed or dynamic based on the ISP: fully-qualified domain names must be used when the IP address is dynamic and are optional when the IP address is static.

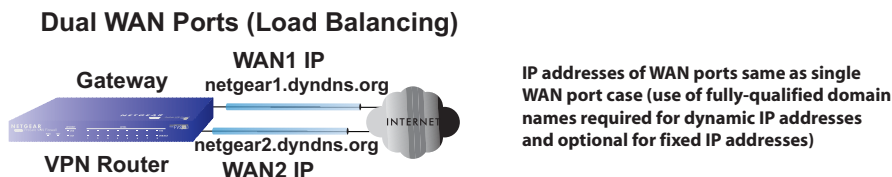


Figure C-8

VPN Road Warrior (Client-to-Gateway)

The following situations exemplify the requirements for a remote PC client with no firewall to establish a VPN tunnel with a gateway VPN firewall:

- Single gateway WAN port
- Redundant dual gateway WAN ports for increased reliability (before and after rollover)
- Dual gateway WAN ports used for load balancing

VPN Road Warrior: Single Gateway WAN Port (Reference Case)

In the case of the single WAN port on the gateway VPN firewall (Figure C-9), the remote PC client initiates the VPN tunnel because the IP address of the remote PC client is not known in advance. The gateway WAN port must act as the responder.

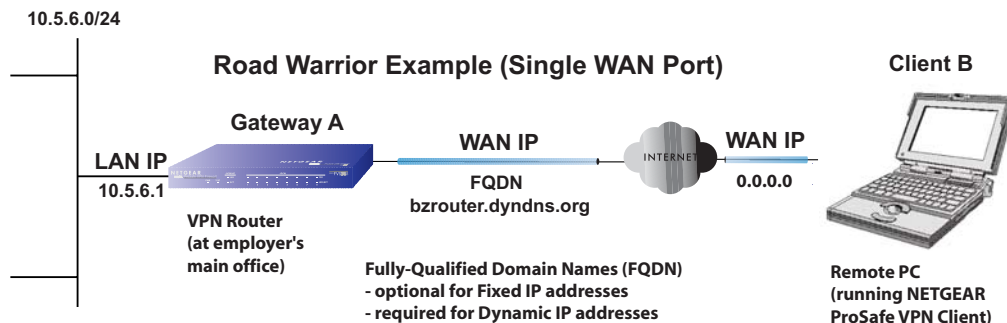


Figure C-9

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, a fully-qualified domain name must be used. If the IP address is fixed, a fully-qualified domain name is optional.

VPN Road Warrior: Dual Gateway WAN Ports for Improved Reliability

In the case of the dual WAN ports on the gateway VPN firewall (Figure C-10), the remote PC client initiates the VPN tunnel with the active gateway WAN port (port WAN1 in this example) because the IP address of the remote PC client is not known in advance. The gateway WAN port must act as a responder.

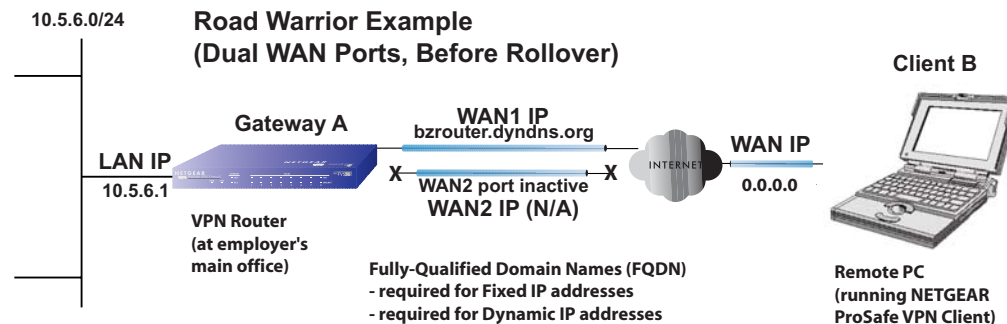


Figure C-10

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but a fully-qualified domain name must always be used because the active WAN port could be either WAN1 or WAN2 (i.e., the IP address of the active WAN port is not known in advance).

After a rollover of the gateway WAN port (Figure C-11), the previously inactive gateway WAN port becomes the active port (port WAN2 in this example) and the remote PC client must re-establish the VPN tunnel. The gateway WAN port must act as the responder.

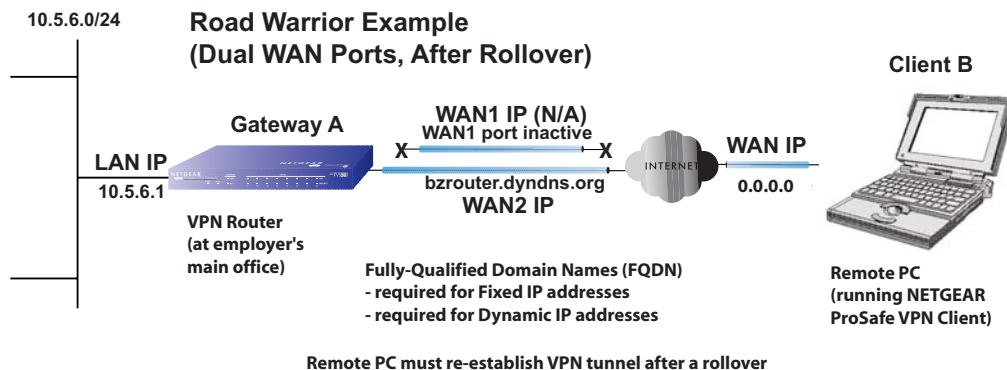
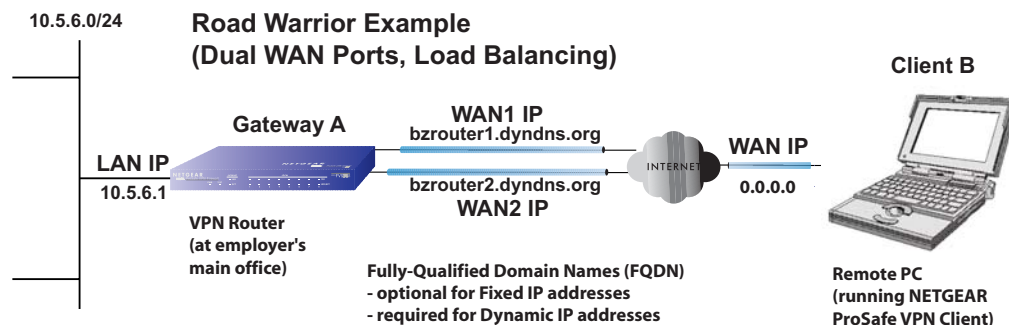


Figure C-11

The purpose of the fully-qualified domain name in this case is to toggle the domain name of the gateway firewall between the IP addresses of the active WAN port (i.e., WAN1 and WAN2) so that the remote PC client can determine the gateway IP address to establish or re-establish a VPN tunnel.

VPN Road Warrior: Dual Gateway WAN Ports for Load Balancing

In the case of the dual WAN ports on the gateway VPN firewall (Figure C-12), the remote PC initiates the VPN tunnel with the appropriate gateway WAN port (i.e., port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the remote PC is not known in advance. The chosen gateway WAN port must act as the responder.

**Figure C-12**

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, a fully-qualified domain name must be used. If an IP address is fixed, a fully-qualified domain name is optional.

VPN Gateway-to-Gateway

The following situations exemplify the requirements for a gateway VPN firewall to establish a VPN tunnel with another gateway VPN firewall:

- Single gateway WAN ports
- Redundant dual gateway WAN ports for increased reliability (before and after rollover)
- Dual gateway WAN ports used for load balancing

VPN Gateway-to-Gateway: Single Gateway WAN Ports (Reference Case)

In the case of single WAN ports on the gateway VPN firewalls ([Figure C-13](#)), either gateway WAN port can initiate the VPN tunnel with the other gateway WAN port because the IP addresses are known in advance.

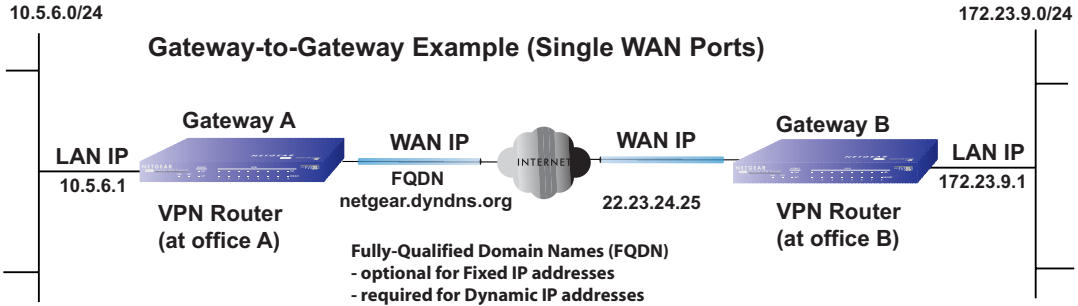


Figure C-13

The IP address of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, a fully-qualified domain name must be used. If an IP address is fixed, a fully-qualified domain name is optional.

VPN Gateway-to-Gateway: Dual Gateway WAN Ports for Improved Reliability

In the case of the dual WAN ports on the gateway VPN firewall (Figure C-14), either of the gateway WAN ports at one end can initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to balance the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance. In this example, port WAN_A1 is active and port WAN_A2 is inactive at Gateway A; port WAN_B1 is active and port WAN_B2 is inactive at Gateway B.

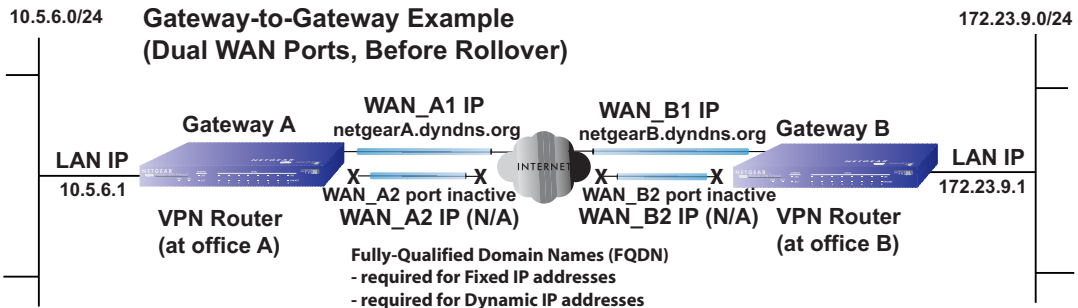


Figure C-14

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but a fully-qualified domain name must always be used because the active WAN ports could be either WAN_A1, WAN_A2, WAN_B1, or WAN_B2 (i.e., the IP address of the active WAN port is not known in advance).

After a rollover of a gateway WAN port (Figure C-15), the previously inactive gateway WAN port becomes the active port (port WAN_A2 in this example) and one of the gateway VPN firewalls must re-establish the VPN tunnel.

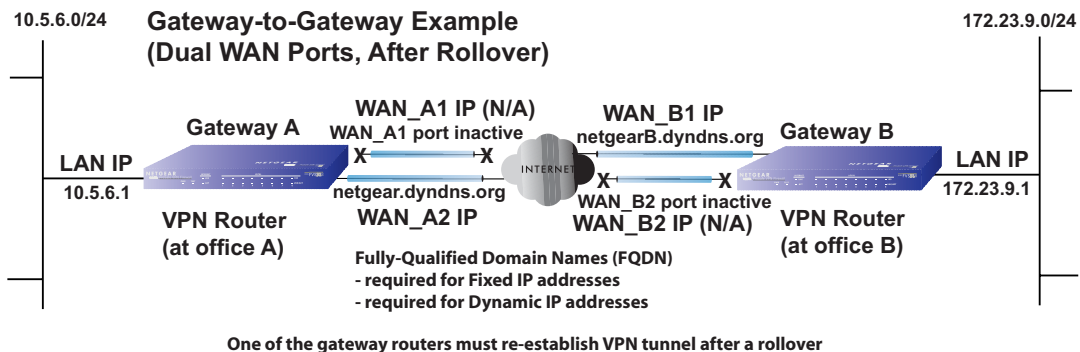


Figure C-15

The purpose of the fully-qualified domain names in this case is to toggle the domain name of the failed-over gateway firewall between the IP addresses of the active WAN port (i.e., WAN_A1 and WAN_A2 in this example) so that the other end of the tunnel has a known gateway IP address to establish or re-establish a VPN tunnel.

VPN Gateway-to-Gateway: Dual Gateway WAN Ports for Load Balancing

In the case of the dual WAN ports on the gateway VPN firewall (Figure C-16), either of the gateway WAN ports at one end can be programmed in advance to initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to manage the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance.

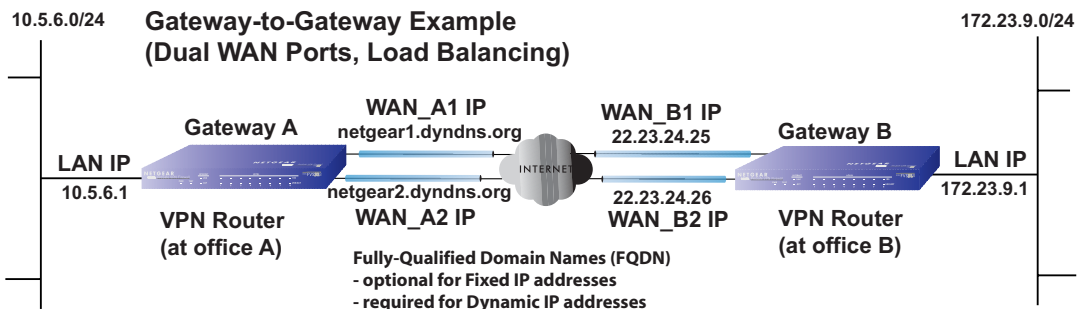


Figure C-16

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, a fully-qualified domain name must be used. If an IP address is fixed, a fully-qualified domain name is optional.

VPN Telecommuter (Client-to-Gateway Through a NAT Router)



Note: The telecommuter case presumes the home office has a dynamic IP address and NAT router.

The following situations exemplify the requirements for a remote PC client connected to the Internet with a dynamic IP address through a NAT router to establish a VPN tunnel with a gateway VPN firewall at the company office:

- Single gateway WAN port
- Redundant dual gateway WAN ports for increased reliability (before and after rollover)
- Dual gateway WAN ports used for load balancing

VPN Telecommuter: Single Gateway WAN Port (Reference Case)

In the case of the single WAN port on the gateway VPN firewall (Figure C-17), the remote PC client at the NAT router initiates the VPN tunnel because the IP address of the remote NAT router is not known in advance. The gateway WAN port must act as the responder.

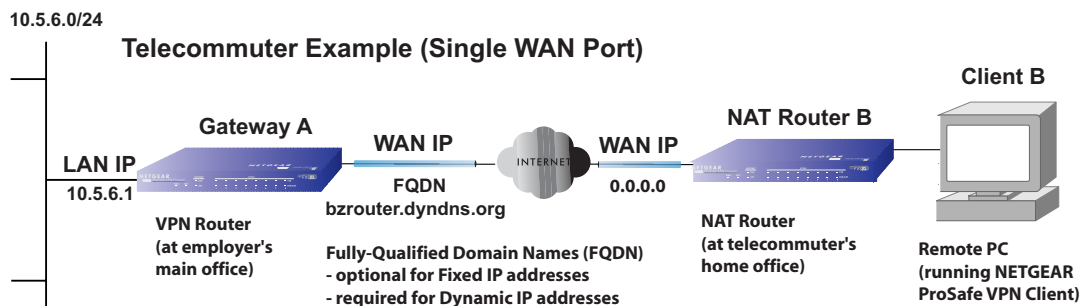


Figure C-17

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, a fully-qualified domain name must be used. If the IP address is fixed, a fully-qualified domain name is optional.

VPN Telecommuter: Dual Gateway WAN Ports for Improved Reliability

In the case of the dual WAN ports on the gateway VPN firewall (Figure C-18), the remote PC client initiates the VPN tunnel with the active gateway WAN port (port WAN1 in this example) because the IP address of the remote NAT router is not known in advance. The gateway WAN port must act as the responder.

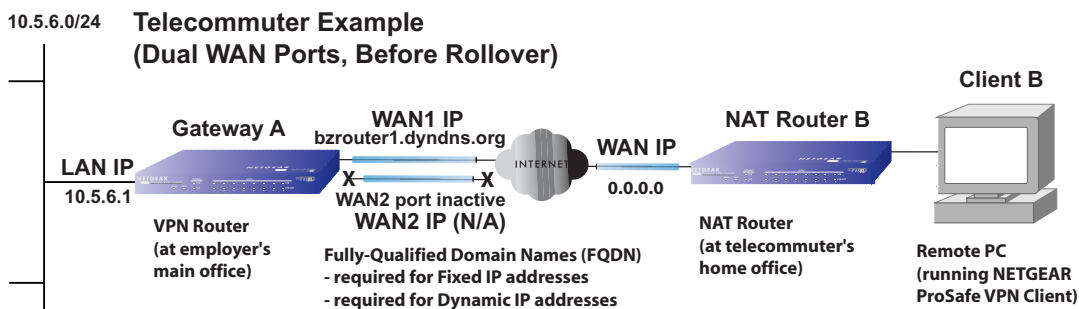


Figure C-18

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but a fully-qualified domain name must always be used because the active WAN port could be either WAN1 or WAN2 (i.e., the IP address of the active WAN port is not known in advance).

After a rollover of the gateway WAN port (Figure C-19), the previously inactive gateway WAN port becomes the active port (port WAN2 in this example) and the remote PC must re-establish the VPN tunnel. The gateway WAN port must act as the responder.

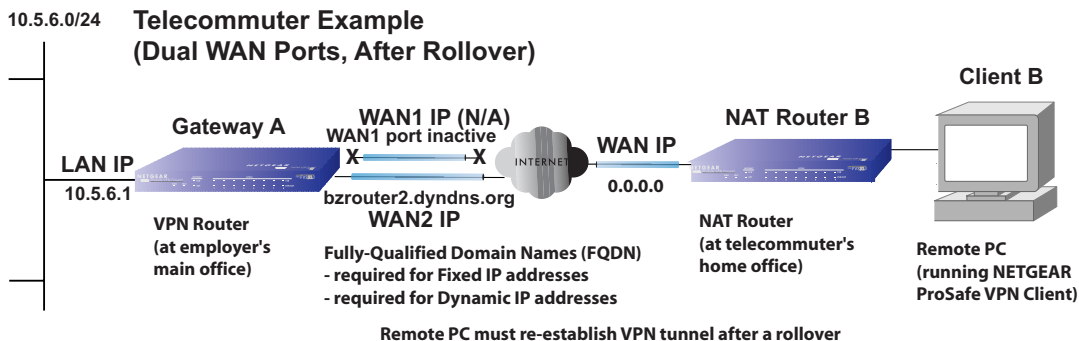


Figure C-19

The purpose of the fully-qualified domain name in this case is to toggle the domain name of the gateway router between the IP addresses of the active WAN port (i.e., WAN1 and WAN2) so that the remote PC client can determine the gateway IP address to establish or re-establish a VPN tunnel.

VPN Telecommuter: Dual Gateway WAN Ports for Load Balancing

In the case of the dual WAN ports on the gateway VPN firewall (Figure C-20), the remote PC client initiates the VPN tunnel with the appropriate gateway WAN port (i.e., port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the remote NAT router is not known in advance. The chosen gateway WAN port must act as the responder.

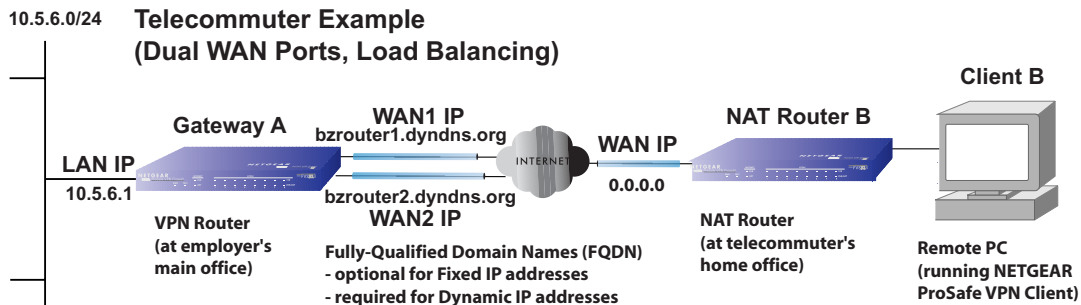


Figure C-20

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, a fully-qualified domain name must be used. If an IP address is fixed, a fully-qualified domain name is optional.

A

- access
 - remote management [6-10](#)
- Active Self Certificates [5-27](#)
- Add DMZ WAN Outbound Services screen [4-12](#)
- Add LAN DMZ Inbound Service screen [4-14](#)
- Add LAN DMZ Outbound Service screen [4-13](#)
- Add LAN WAN Inbound Service [4-10](#)
- Add LAN WAN Outbound Service screen [4-9](#)
- Add Mode Config Record screen [5-38](#)
- Add Protocol Binding
 - Destination Network [2-13](#)
 - Service [2-13](#)
- address reservation [3-9](#)
- Advanced Options
 - MTU Size [2-19](#)
 - Port Speed [2-19](#)
 - Router's MAC Address [2-19](#)
- Allowing Videoconference from Restricted Addresses
 - example of [4-17](#)
- Attack Checks
 - about [4-14](#)
- Attack Checks screen [4-15](#)
- Authentication Algorithm
 - IKE Policy [5-12](#)
- Auto Detect [2-3](#)
- Auto Uplink [1-3](#)
- Auto-Rollover
 - configuration of [2-11](#)
 - definition of [2-10](#)
 - Dual WAN ports [5-1](#)
 - restoring WAN interface [2-12](#)
 - use with DDNS [2-16](#)
 - Using WAN port [2-11](#)

B

- Back up settings [6-13](#)
- backup and restore settings [6-14](#)
- bandwidth capacity [6-1](#)
 - LAN side [6-1](#)
 - Load balancing mode [6-1](#)
 - Rollover mode [6-1](#)
 - WAN side [6-1](#)
- BigPond Cable [2-4, 2-5](#)
 - Internet connection [2-6](#)
- Block Sites [1-2](#)
 - Content Filtering [4-25](#)
 - reducing traffic [6-4](#)
- Block Sites screen [4-25](#)
- Block TCP Flood [4-14](#)
- block traffic
 - with schedule [4-24](#)
- Blocking Instant Messenger
 - example of [4-20](#)

C

- CA
 - about [5-27](#)
- Cat5 cable [C-3](#)
- Certificate Authority. See CA.
- Classical Routing
 - definition of [2-10](#)
- command line interface [6-11](#)
- configuration
 - automatic by DHCP [1-4](#)
- connecting the VPN firewall [2-1](#)
- Connection Status
 - VPN Tunnels [5-13](#)
- Content [4-25](#)

- Content Filtering *4-1*
 - about *4-25*
 - Block Sites *4-25*
 - enabling *4-25*
 - firewall protection, about *4-1*
- content filtering *1-2, 4-1*
- crossover cable *1-3, 7-2*
- Customized Service
 - editing *4-23*
- customized service
 - adding *4-22*
- Customized Services
 - adding *4-2, 4-21*
- D**
- Date
 - setting *6-16*
 - troubleshooting *7-7*
- Daylight Savings Time
 - adjusting for *6-16*
- DDNS
 - about *2-15*
 - configuration of *2-16*
 - links to *2-17*
 - providers of *2-15*
 - services, examples *2-17*
- DDNS providers
 - links to *2-17*
- default configuration
 - restoring *7-7*
- default IP Address *1-9*
- default password *1-9, 2-2*
- default user name *1-9, 2-2*
- denial of service attack *4-14, 4-15*
- Denial of Service. See DoS.
- Destination Network
 - Add Protocol Binding *2-14*
- DHCP *2-4*
- DHCP Address Pool *3-3*
- DHCP IP Address pool *3-1*
- DHCP log
 - monitoring *6-27*
- DHCP server
 - about *3-1*
 - configuring secondary IP addresses *3-5*
- diagnostics
 - DNS lookup *6-27*
 - packet capture *6-27*
 - ping *6-27*
 - rebooting *6-27*
 - routing table *6-27*
- Diagnostics screen *6-27*
- Diffie-Hellman Group
 - IKE Policy *5-12*
- Disable DHCP Server *3-1, 3-3*
- DMZ
 - about *3-10*
 - firewall security *3-10*
- DMZ Port
 - increasing traffic *6-7*
- DMZ port *1-3*
 - setting up *3-10*
- DMZ Setup screen *3-10*
- DMZ WAN Inbound Rule
 - example of *4-19*
- DMZ WAN Rule
 - example of *4-17*
- DMZ WAN Rules
 - about *4-10*
 - modifying *4-12*
- DMZ WAN Rules screen *4-10*
- DNS
 - definition of *2-7*
- DNS addresses *2-7*
- DNS lookup *2-11*
- DNS Proxy *1-4*
- DNS queries
 - Auto-Rollover *2-11*
- Domain Name
 - router *3-3*
- Domain Name Blocking *4-25*
- Domain Name Servers. See DNS.
- DoS

- about protection *1-2*
- Dual WAN
 - configuration of *2-10*
- Dual WAN Port
 - inbound traffic *C-8*
 - load balancing, inbound traffic *C-9*
- Dual WAN Port systems
 - VPN Tunnel addresses *5-1*
- Dual WAN Ports
 - features of *1-2*
 - network planning *C-1*
- Dual WAN ports
 - Auto-Rollover, configuration of *2-11*
 - Load Balancing, configuration of *2-13*
- Dynamic DNS
 - configuration of *2-15*
- Dynamic DNS Configuration screen *2-16*
- Dynamic DNS. See DDNS
- DynDNS.org *2-15*

E

- Edge Device *5-32*
 - XAUTH, with ModeConfig *5-40*
- Edit Group Names *2-14, 3-9*
- Edit IKE Policy screen *5-6*
- Edit Protocol Binding *2-14*
- Edit VPN Policy screen *5-9*
- E-mail alerts *4-32*
- e-mail logs
 - enabling notification *4-32*
- E-mail Server address *4-33*
- Enable DHCP Server *3-3*
- Enable DHCP server *3-1*
- Enable DNS Proxy *3-3*
- Enable the DHCP Server
 - DMZ port *3-11*
- Encapsulating Security Payload
 - VPN Policy *5-13*
- Ending IP Address
 - DHCP Address Pool *3-3*

- Ethernet, Auto Uplink *1-3*
- Event Logs
 - emailing of *4-31*
- Extended Authentication. See XAUTH.

F

- factory default login *1-9*
- factory default settings
 - revert to *6-13*
- firewall
 - connecting to the Internet *2-1, C-3*
 - features *1-1, 1-2, 1-3, 1-4*
 - front panel *1-6*
 - rear panel *1-8*
 - technical specifications *A-1*
 - viewing activity *6-25*
- Firewall Log
 - Field Description *4-35*
- Firewall Logs
 - emailing of *4-31*
 - setting up *4-32*
 - viewing *4-34*
- Firewall Logs & E-mail screen *4-31, 4-32, 6-19*
- Firewall Protection
 - Content Filtering, about *4-1*
- firewall protection *4-1*
- firmware
 - downloading *6-15*
 - upgrade *6-15*
- Fixed IP *2-4*
- Fixed IP Address *3-7*
- FQDN *2-16*
- fully qualified domain name. See FQDN.
- FVX538
 - features of *1-1*

G

- Gateway VPN Tunnel
 - creating *5-4*
- Gigabit Switch port *1-1*
- Group Names

editing 3-9

Groups and Hosts screen 3-7, 3-9, 3-10

groups, managing 3-6

H

hardware requirements C-3

Hosting A Local Public Web Server

example of 4-16

hosts, managing 3-6

I

Iego.net 2-15

IGP 3-13

IKE Policies

management of 5-11

IKE Policies screen 5-9

IKE Policy

about 5-10

ModeConfig, configuring with 5-39

XAUTH, adding to 5-32

Inbound Rules

default definition 4-2

field descriptions 4-5

order of precedence 4-7

Port Forwarding 4-2, 4-4

rules for use 4-4

inbound rules 4-4

example 4-17

Inbound Service Rule

modifying 4-8

Inbound Services

field descriptions 4-5

inbound traffic C-6, C-8

dual WAN ports C-8, C-9

single WAN port reference case C-8

increasing traffic 6-5

DMZ Port 6-7

Port Forwarding 6-5

Port Triggering 6-6

VPN Tunnels 6-7

installation 1-4

Installation, instructions for 2-1

Interior Gateway Protocol. See IGP.

Internet

configuration requirements C-3, C-4, C-5

configuring the connection manually 2-5

connecting to 2-1

Internet connection

configuring 2-2

manual configuration 2-5

Internet service

connection types 2-3

Internet Service Provider. See ISP.

Internet Traffic Statistics 6-18

IP Address

router default 3-2

IP addresses

auto-generated 7-3

DHCP address pool 3-1

how to assign 3-1

multi home LAN 3-4

reserved 3-9

IP Subnet Mask

router default 3-2

IPsec 4-15

IPSec Connection Status screen 6-25

IPSec Host 5-32, 5-33

IPsec Host

XAUTH, with ModeConfig 5-40

ISP connection

troubleshooting 7-4

K

Keep Connected

Idle Timeout 2-6

Idle Timeout 2-6

Keyword Blocking 4-25

applying 4-25

Keyword Filtering 1-3

Known PCs and Devices

list of 3-7

L

L2TP 4-15

LAN

configuration 3-1

using LAN IP setup options 3-2

LAN DMZ Inbound Services

adding rule 4-14

LAN DMZ Outbound Services

adding rule 4-13

LAN DMZ Rules 4-12

LAN DMZ Rules screen 4-12

LAN DMZ service rule

modifying 4-13

LAN Security Checks 4-15

LAN Setup screen 3-2, 6-27

LAN side

bandwidth capacity 6-1

LAN WAN Inbound Rule

example of 4-16, 4-17, 4-19

LAN WAN Inbound Services Rules

about 4-10

add 4-10

LAN WAN Outbound Rule

example of 4-20

LAN WAN Outbound Rules

about 4-9

LAN WAN Rule

example of 4-17

LAN WAN Rules

default outbound 4-7

LAN WAN Rules screen 4-7

LEDs

explanation of 1-6

troubleshooting 7-1, 7-2

Load Balancing

configuration of 2-13

definition of 2-10

use with DDNS 2-16

view protocol bindings 2-13

Load balancing mode

bandwidth capacity 6-1

logging in

default login 2-1

logging into the router

default login 1-10

M

MAC Address

format 3-8

format of 4-28

MAC address 7-6

configuring 2-4, 2-5

format of 2-19

spoofing 7-5

MAC addresses

blocked, adding 4-27

Maximum Failover 2-12

ModeConfig 5-37

about 5-37

assigning remote addresses, example 5-37

Client Configuration 5-41

IKE Policies menu, configuring 5-38

menu, configuring 5-38

testing Client 5-45

monitoring devices 6-20

by DHCP Client Requests 6-21

by Scanning the Network 6-21

MTU Size 2-19

Multi Home LAN IPs

about 3-4

multi home LAN IPs 3-4

N

NAS

Identifier 5-36

NAT

definition of 2-10

features of 1-3

firewall, use with 4-1

Network Access Server. See NAS.

Network Address Translation. See NAT.

Network Address Translation. See NAT.

Network Configuration 2-11

network configuration requirements *C-3*

Network Database

about *3-6*

advantages of *3-6*

fields *3-7*

Network Database Group Names screen *3-9*

network planning

Dual WAN Ports *C-1*

Network Time Protocol. See NTP.

newsgroup *4-25*

NTP *6-16*

troubleshooting *7-7*

NTP Servers

custom *6-17*

default *6-16*

NTP servers

setting *6-16*

O

Outbound Rules

default definition *4-2*

field descriptions *4-3*

order of precedence *4-7*

service blocking *4-2*

outbound rules *4-2*

Outbound Service Rule

modifying *4-8*

Outbound Services

field descriptions *4-3*

Outbound Services Rules

adding *4-9*

P

package contents *1-5*

passwords and login timeout

changing *6-8*

passwords,restoring *7-7*

performance management *6-1*

Ping

responding to *2-5*

troubleshooting TCP/IP *7-5*

Ping On Internet Ports *4-14*

Ping to an IP address

Auto-Rollover *2-11*

Ping to this IP address *2-12*

planning

inbound traffic *C-6, C-8*

VPNs *C-6*

port filtering

service blocking *4-2*

Port Forwarding

Inbound Rules *4-2, 4-4*

increasing traffic *6-5*

rules, about *4-4*

port forwarding *6-5*

Port Mode *2-11*

port numbers *4-21*

Port Speed *2-19*

Port Triggering

about *4-28*

adding a rule *4-29*

increasing traffic *6-6*

modifying a rule *4-31*

rules of use *4-28*

port triggering *6-6*

status *6-22*

Port Triggering screen *4-29, 6-22*

ports

explanation of WAN and LAN *1-6*

PPP over Ethernet. See PPPoE.

PPPoE *1-4, 2-3, 2-5*

Internet connection *2-6*

PPTP *2-3, 2-5, 4-15*

precedence, order of for rules *4-21*

protocol numbers

assigned *4-21*

protocols

Routing Information Protocol *1-3*

Q

QoS *4-2*

about *4-23*

priority definitions 4-23
 shifting traffic mix 6-7
 SIP 2.0 support 1-1

Quality of Service. See QoS

Quality of Service. See Qos.

R

rack mounting 1-9

rack mounting hardware 1-9

RADIUS Server
 configuring 5-35

RADIUS-CHAP 5-31, 5-33
 AUTH, using with 5-32

RADIUS-PAP 5-31
 XAUTH, using with 5-32

reducing traffic 6-2

Block Sites 6-4
 Service Blocking 6-2
 Source MAC Filtering 6-4

remote management 6-10
 access 6-10
 configuration 6-10

remote users
 assigning addresses 5-37
 ModeConfig 5-37

requirements
 hardware C-3

Reserved IP Address 3-7

Reserved IP address
 restrictions 3-7

Reserved IP Addresses 3-9

Restore saved settings 6-13

Return E-mail Address 4-33

RFC 1349 4-23

RFC1700
 protocol numbers 4-21

RIP 3-13
 about 3-13
 configuring parameters 3-13
 static routes, use with 3-13
 versions of 3-14

RIP Configuration screen 3-13

Rollover mode
 bandwidth capacity 6-1

router
 upgrade software 6-16

router administration
 tips on 4-35

router broadcast
 RIP, use with 3-13

Router Status 2-11

Router Status screen 6-23

Router Upgrade
 about 6-15

Router's MAC Address 2-19

Routing Information Protocol 1-3

Routing Information Protocol. See RIP.

Routing screen 3-12

rules
 blocking traffic 4-1
 inbound 4-4
 inbound example 4-17
 order of precedence 4-21
 outbound 4-2
 service blocking 4-2
 services-based 4-2

running tracer 6-11

S

schedule
 blocking traffic 4-24

Schedule 1 screen 4-24

secondary IP addresses
 DHCP, use with 3-5

Secondary LAN IPs
 see Multi Home LAN IPs 3-4

Security
 features of 1-3

Self Certificate Request
 generating 5-28

Send To E-mail Address 4-33

Service

- Add Protocol Binding 2-14
 - Service Based Rules 4-2
 - Service Blocking
 - reducing traffic 6-2
 - service blocking 4-2
 - Outbound Rules 4-2
 - port filtering 4-2
 - service numbers
 - common protocols 4-21
 - Services screen 4-21, 4-22
 - Setting Up One-to-One NAT Mapping
 - example of 4-17
 - Settings Backup & Upgrade screen 6-13
 - Settings Backup and Firmware Upgrade 6-14
 - Simple Network Management Protocol. See SNMP.
 - Single WAN Port
 - inbound traffic C-8
 - sniffer 7-3
 - SNMP
 - about 6-11
 - configuring 6-12
 - global access 6-12
 - host only access 6-12
 - subnet access 6-12
 - SNMP screen 6-12
 - Source MAC Filter screen 4-27
 - Source MAC Filtering
 - enabling 4-27
 - reducing traffic 6-4
 - Source Network
 - Add Protocol Binding 2-14
 - Specifying an Exposed Host
 - example of 4-19
 - spoof MAC address 7-5
 - Starting IP Address
 - DHCP Address Pool 3-3
 - Stateful Packet Inspection
 - firewall, use with 4-1
 - stateful packet inspection 1-2
 - Static IP 2-4
 - static IP 2-6
 - Static Route
 - example of 3-15
 - Static Routes
 - about 3-12
 - static routes
 - add or edit 3-12
 - configuring 3-12
 - example 3-15
 - Stealth Mode 4-14
 - SYN flood 4-14
 - SysLog Facility Message Levels 4-33
 - SysLog Server
 - IP Address 4-33
- ## T
- TCP/IP
 - network, troubleshooting 7-5
 - Test Period 2-12
 - Time
 - setting 6-16
 - troubleshooting 7-7
 - time
 - daylight savings, troubleshooting 7-7
 - Time Zone
 - setting of 6-16
 - Time Zone screen 6-16
 - ToS. See QoS.
 - tracert
 - use with DDNS 6-11
 - traffic
 - increasing 6-5
 - reducing 6-2
 - Traffic by Protocol 6-18
 - traffic management 6-8
 - Traffic Meter 2-7
 - traffic meter 2-4
 - programming 2-7
 - WAN2 ISP settings 2-5
 - Traffic Meter screen
 - router monitoring 6-17
 - Traffic Meter Settings 2-9

- definitions 2-9
 - Trend Micro
 - enabling 3-15
 - Office Scan Server 3-16
 - OfficeScan client, exclusion list 3-16
 - requirements for use 3-15
 - Trend Micro integration 1-4
 - Trend Micro screen 3-16
 - Trend Micro security 1-4
 - troubleshooting 7-1
 - browsers 7-3
 - configuration settings, using sniffer 7-3
 - defaults 7-3
 - ISP connection 7-4
 - NTP 7-7
 - testing your setup 7-6
 - Web configuration 7-2
 - Trusted Certificates 5-27
 - Trusted Domains
 - building list of 4-26
 - TZO.com 2-15
- ## U
- UDP flood 4-15
 - Use Default Address 2-5
 - User Database 5-32
 - adding user 5-34
 - editing user 5-35
 - User Database screen 5-34
- ## V
- view protocol bindings
 - Load Balancing 2-13
 - viewing logs 6-19
 - VPN
 - gateway to gateway, about C-14
 - gateway-to-gateway, Dual gateway C-15
 - gateway-to-gateway, single gateway C-14
 - Load Balancing, examples of C-11
 - load balancing, with dual WAN ports C-7
 - Road Warrior, dual gateway C-12
 - Road Warrior, examples of C-11
 - Road Warrior, single gateway C-12
 - Rollover, examples of C-10
 - rollover, with dual WAN ports C-7
 - telecommuter, about C-17
 - telecommuter, Dual gateway C-18
 - telecommuter, single gateway C-18
 - VPN Client
 - configuring 5-7
 - configuring PC, example 5-22
 - VPN Wizard example 5-20
 - VPN firewall
 - connecting 2-1
 - VPN Logs
 - monitoring 6-26
 - VPN Logs screen 6-26
 - VPN Pass through 4-15
 - VPN Policies screen 5-5, 5-9
 - VPN Policy
 - Auto 5-12
 - Auto generated 5-10
 - field definitions 5-13
 - Manual 5-12
 - VPN Tunnel
 - Client Policy 5-7
 - FVS338, configuring, example of 5-19
 - FVX538 configuration, example 5-14
 - load balancing mode 5-1
 - rollover mode 5-1
 - VPN Tunnel addresses
 - Dual WAN Port systems 5-1
 - VPN Tunnel Connection
 - monitoring status 6-25
 - VPN Tunnels
 - Connection Status 5-13
 - increasing traffic 6-7
 - L2TP 4-15
 - VPN tunnels
 - about 5-1
 - IPsec 4-15
 - PPTP 4-15
 - VPN Wizard
 - Gateway tunnel 5-4
 - VPN Client, configuring 5-7
 - VPN Wizard Default Values 5-5

VPNs *C-6, C-10*
 about *C-10*
 creating a VPN Gateway connection *5-14*
 gateway-to-gateway *C-14, C-15, C-17*
 road warrior *C-11, C-12, C-13*
 telecommuter *C-18, C-20*
 viewing VPN tunnel status *6-25*

W

WAN
 configuring Advanced options *2-18*
 configuring WAN Mode *2-10*
WAN Failure Detection Method *2-10, 2-11*
WAN Mode *2-11*
WAN Mode setup *5-2*
WAN Port 1 status *2-4*
WAN Ports
 monitoring status *6-24*
WAN ports
 status of *2-11*
WAN Security Check
 about *4-14*
WAN Settings screen *2-18*
WAN side
 bandwidth capacity *6-1*
WAN Status *2-4*
WAN1 Advanced Options *2-18*
WAN1 ISP Settings
 manual setup *2-5*
WAN1 ISP Settings screen *2-2*
WAN1 Protocol Bindings *2-13*
WAN1 Protocol Bindings screen *2-14*
WAN1 Traffic Meter *2-7*
WAN2 ISP
 settings *2-5*
WAN2 ISP Settings
 manual setup *2-7*
WAN2 Protocol Bindings *2-14*
WAN2 Protocol Bindings screen. *2-14*
WAN2 Traffic Meter *2-8*

Web Components *4-25*
 blocking *4-25*
 filtering, about *4-25*
Web configuration
 troubleshooting *7-2*
WinPoET *2-6*

X

XAUTH
 IPSec Host *5-32*
 types of *5-31*